



HP Access Control (HP AC)

Getting Started Guide

© Copyright 2014 Hewlett-Packard
Development Company, L.P.

Microsoft, Windows, and Windows NT are U.S.
registered trademarks of Microsoft
Corporation.

July 2014

**Confidential computer software. Valid
license from HP required for possession, use
or copying. Consistent with FAR 12.211 and
12.212, Commercial Computer Software,
Computer Software Documentation, and
Technical Data for Commercial Items are
licensed to the U.S. Government under
vendor's standard commercial license.**

The information contained herein is subject to
change without notice. The only warranties for
HP products and services are set forth in the
express warranty statements accompanying
such products and services. Nothing herein
should be construed as constituting an
additional warranty. HP shall not be liable for
technical or editorial errors or omissions
contained herein.

Table of contents

1 Introduction	1
2 Prerequisites	2
3 License tile	4
4 Settings tile	5
4.1 Database tab	5
4.2 Device tab	6
4.3 Email tab	9
4.4 IIS tab	11
4.5 SPPE tab	15
4.6 SPP Enterprise tab	17
4.7 Alias tab	21
4.8 Agent tab	22
4.9 Print server tab	24
4.10 IPM tab	25
4.11 FDT tab	28
5 Devices tile	29
5.1 Scan the network for printers	32
5.2 Scan the network for XT devices	33
5.3 Manually add a device	34
5.4 Delete a device from the device list	34
5.5 Import/Export device data	34
5.6 Organize and manage devices	34
5.7 Install and configure components on HP FutureSmart and non-FutureSmart devices	36
5.8 Configure components on HP Officejet Pro printers	38
5.8.1 Unregister an Officejet Pro printer	41
5.9 Configure components on HP S900 series devices	43
5.9.1 Pull printing at the device	49
5.10 Install and configure components on Lexmark devices	50
5.10.1 Install HP Access Control (HP AC) Lexmark Applications	52
5.10.2 Configure AC Lexmark Applications	53
5.10.3 Lexmark device security settings	53
5.10.4 Using the AC Lexmark applications	54

- 5.11 Install and configure components on Xerox devices 56
 - 5.11.1 Configure AC Xerox Applications 57
 - 5.11.2 Using the AC Xerox Applications 58
- 5.12 Configure XT devices 59
 - 5.12.1 Pull print using XT card readers 59
- 6 Print server tile 60
- 7 Server Information tile 61
- 8 HP Access Control (HP AC) Print Client 62

List of tables

Table 5-1 Supported HP OfficeJet Pro printers and firmware 38

Table 5-2 Supported printers 56

List of figures

Figure 1-1	Home screen	1
Figure 2-1	Database setup	2
Figure 2-2	Retrieve user data	2
Figure 2-3	Push mode setup	3
Figure 2-4	Device password setup	3
Figure 2-5	Web service setup	3
Figure 3-1	License tile	4
Figure 4-1	Settings file menu	5
Figure 4-2	Database tab	6
Figure 4-3	Device tab	7
Figure 4-4	Device settings	7
Figure 4-5	Tracking settings	8
Figure 4-6	OPS server settings	8
Figure 4-7	SNMP settings	8
Figure 4-8	Concurrent connections	9
Figure 4-9	Email tab	10
Figure 4-10	POP3 IMAP settings	10
Figure 4-11	SMTP settings	11
Figure 4-12	IIS tab	12
Figure 4-13	Web service settings	12
Figure 4-14	CORS trusted sites	13
Figure 4-15	Agent license service settings	14
Figure 4-16	Push mode	14
Figure 4-17	IPM authentication	14
Figure 4-18	SPPE settings	15
Figure 4-19	Pull Printing settings	16
Figure 4-20	QR code	16
Figure 4-21	Email section	17
Figure 4-22	Job Accounting	17
Figure 4-23	SPP Enterprise settings	18
Figure 4-24	Server Information settings	18
Figure 4-25	Pull print queues settings	19
Figure 4-26	Options	20
Figure 4-27	Email settings	20
Figure 4-28	Alias tab	21
Figure 4-29	Alias window	22

Figure 4-30	Agent tab	22
Figure 4-31	HP install files	23
Figure 4-32	Lexmark install	23
Figure 4-33	IRM quota web service	23
Figure 4-34	Print server tab	24
Figure 4-35	IPM tab	25
Figure 4-36	IPM web service settings	25
Figure 4-37	Print activity log	25
Figure 4-38	Notification desktop client	26
Figure 4-39	Cost per page	27
Figure 4-40	User grouping	27
Figure 4-41	FDT tab	28
Figure 5-1	Devices tile	29
Figure 5-2	Configure window	30
Figure 5-3	Devices dropdown menu	31
Figure 5-4	QR code	31
Figure 5-5	IP range	32
Figure 5-6	Devices menu	33
Figure 5-7	IP range window	33
Figure 5-8	Add devices	34
Figure 5-9	Add device groups	35
Figure 5-10	Group devices	35
Figure 5-11	Filter devices	36
Figure 5-12	Device install	37
Figure 5-13	Configure device	38
Figure 5-14	Default website properties	39
Figure 5-15	Assign an existing certificate	39
Figure 5-16	Select certificate	40
Figure 5-17	Edit bindings	40
Figure 5-18	SSL certificate	41
Figure 5-19	OfficeJet configure	41
Figure 5-20	Unregister officeJet	42
Figure 5-21	Card Reader settings	44
Figure 5-22	Insert card reader prompt	44
Figure 5-23	Card reader registration	45
Figure 5-24	Default settings	46
Figure 5-25	Home screen settings	47
Figure 5-26	Home screen registration	47
Figure 5-27	Custom image	47
Figure 5-28	Standard Application settings	48
Figure 5-29	Standard Application registration	48

Figure 5-30	External accounting application settings	49
Figure 5-31	Apps	50
Figure 5-32	Lexmark application	52
Figure 5-33	Lexmark welcome	55
Figure 5-34	Lexmark swipe	55
Figure 5-35	Lexmark select	55
Figure 5-36	Xerox application	57
Figure 5-37	Xerox welcome	58
Figure 5-38	Xerox documents	58
Figure 6-1	Print server tile	60
Figure 7-1	Server Information tile	61
Figure 8-1	HP AC Print Client connection	62
Figure 8-2	HP AC Print Client configuration	63

1 Introduction

This guide is intended for administrators with experience using Windows servers. The following chapters explain how to use the HP Access Control (HP AC) configuration tool and introduce you to the process of configuring HP Access Control (HP AC) solutions on printers.

To open the HP Access Control (HP AC) configuration tool, go to **Start > All Programs > HP Access Control**, then click **HP AC Configuration utility**.

The HP Access Control (HP AC) configuration tool consists of components organized as tiles on the home screen.

Figure 1-1 Home screen



NOTE: The tiles may vary, depending on what HP Access Control (HP AC) components are installed on the server.

Click a tile from the HP Access Control (HP AC) home screen to use the component. Return to the home screen at any time by clicking the back button in the top left corner.

This guide provides information about the License, Settings, Devices, Print Server, and Server Information tiles. For more information about HP Access Control (HP AC) components, see the individual component guides.

To view the individual component guides, click a component tile. Go to the **Help** menu, then click **Administrator Guide** or **User Guide**.

2 Prerequisites

Before using HP Access Control (HP AC) components, make sure to complete the following steps.

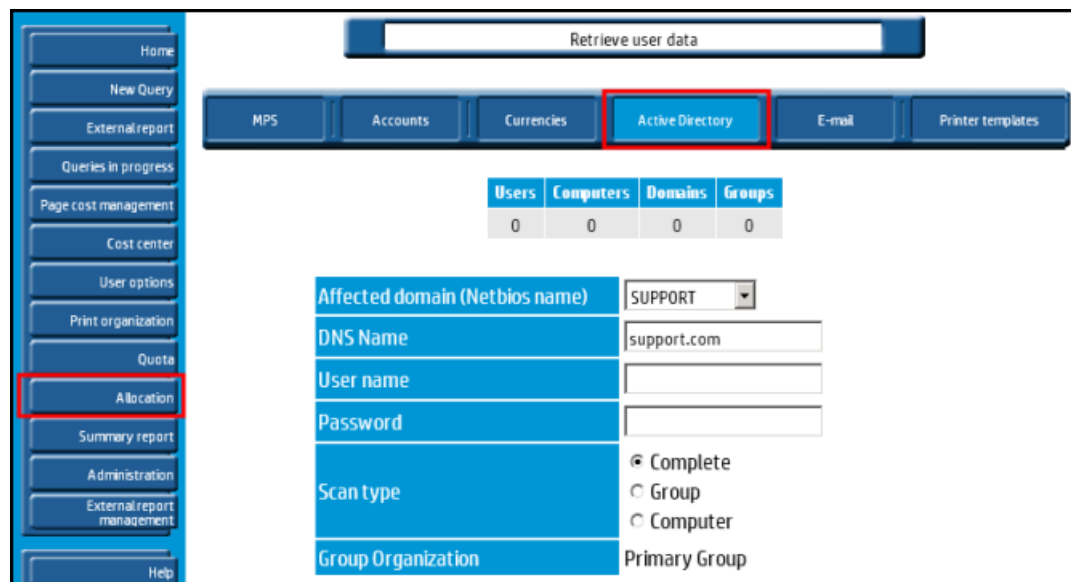
- If you will be using Job Accounting, go to the **Settings** tile > **Database** tab > **Database Configuration** section and verify the SQL server connection settings. Click **Test** to test the connection to the Job Accounting database in SQL. Click **Apply** to apply the settings.

Figure 2-1 Database setup



- If you will be using Job Accounting, you must scan the Active Directory domain to allow for accurate user tracking. Go to the **Job Accounting** tile > **Administration** > **Active Directory** > **Retrieve User Data**. Enter the correct information regarding your domain and administrator credentials, then click the **Go** button. For more information, see the *HP Access Control (HP AC) Job Accounting User Guide*.

Figure 2-2 Retrieve user data



- If you will be using Agent or print server to send tracking information to the Job Accounting server, go to the **Settings** tile > **IIS** tab > **Push mode** section. Select a transfer protocol to auto-upload, or push, tracking data. Click **Test** to test the connection to the Job Accounting server. Click **Apply**.

Figure 2-3 Push mode setup

The screenshot shows the 'Push mode' configuration window. At the top, there is a navigation bar with tabs: Database, Device, Email, IIS, SPPE, Agent, Print server, and IPM. The 'Push mode' section contains the following fields: 'HTTP/FTP' with a dropdown menu set to 'http', 'Port' with a text box containing '80', 'Login' with a text box containing 'domain\user', 'Password' with a masked text box (*****), and 'Interval (minutes)' with a text box containing '0'. At the bottom right, there are two buttons: 'Test' and 'Apply', both of which are highlighted with red rectangular boxes.

- If you will be configuring devices, go to the **Settings** tile > **Device** tab > **Device** section. Enter a device password in the Administrator password field. This device password must match the device passwords in all printers. Click **Apply**.

Figure 2-4 Device password setup

The screenshot shows the 'Device' configuration window. At the top, there is a navigation bar with tabs: Database, Device, Email, IIS, SPPE, Agent, Print server, and IPM. The 'Device' section contains the following fields: 'Administrator user name' with a text box containing 'admin', 'Administrator password' with a masked text box (*****), and 'Certificate' with a text box containing 'C:\Program Files\Hewlett-Packard\HP Access Control\10.0.3.11.cer'. At the bottom right, there is an 'Apply' button, which is highlighted with a red rectangular box.

- If you will be using Job Accounting, IPM, Secure Pull Print, Secure Pull Print Express, Secure Pull Print Enterprise, or IRM, go to the **Settings** tile > **IIS** tab > **Web service** section and verify the server information. Click **Test** to test the connection. Click **Apply**.

Figure 2-5 Web service setup

The screenshot shows the 'Web service' configuration window. At the top, there is a navigation bar with tabs: Database, Device, Email, IIS, SPPE, Agent, Print server, and IPM. The 'Web service' section contains the following fields: 'Server name' with a text box containing 'WB2008.tech.com', 'Server IP' with a text box containing '10.0.0.63', and two checkboxes: 'Encrypt all web communication (devices)' (unchecked) and 'Use server name instead of IP (devices)' (checked). At the bottom right, there are two buttons: 'Test' and 'Apply', both of which are highlighted with red rectangular boxes.




3 License tile

The License tile shows your server license number, Activation Keys for installed components and expiration dates of licenses.

Figure 3-1 License tile

The screenshot shows the HP License tile interface. At the top, there is an ID key field with the value 'BEFAAE07' and a note: 'To contact a licensing customer support center, go to <http://licensing.hp.com> and click on the "contact HP licensing" link on the left. The form provided allows you to send requests to the licensing support team.' Below this, there are five license sections:

- HPAC Secure Pull Print Express:** Activation key: 6F5EF5285F33E1F0C2011E93, 0/10 device(s), Expiration date: 9/22/2013.
- HPAC Agent:** Activation key: 158CF40DFE570032CEB9F627B9C1199, IPA: 0/1000, Expiration date: 9/22/2013, DBA: 0/1000, PIC: 0/1000, IRM: 0/1000.
- HPAC Device Analysis:** Activation key: 0F60937B53C7BB46E85A2AFD, Devices: Unlimited, Expiration date: 9/22/2013.
- HPAC IPM:** Activation key: 70895723A4AAB099C4C6CAC6, 0/10 device(s), Expiration date: 9/22/2013.
- HPAC Job Accounting:** Activation key: (empty), Evaluation version, Expiration date: 9/22/2013.

-  **NOTE:** Information in the License tile may vary depending on what components of HP Access Control (HP AC) are installed on the server.
-  **NOTE:** The License tile is highlighted red on the HP Access Control (HP AC) home screen if a component license is expired.
-  **NOTE:** The Secure Pull Print Express license resets after 24 hours. This allows for users to pull print at new devices every day.

The ID key field contains the server license number that identifies your server for the HP Licensing Support team. To receive Activation Keys for components, you need to contact the HP licensing customer support center:


1. Go to the HP licensing customer support center at <http://licensing.hp.com>.
2. Click **Contact HP Licensing** on the left.
3. Fill in all required fields. In the **Your comments** field, make sure to include your server license number. Then submit the form.

After your license request is processed, you will receive an email containing Activation Keys. Copy the component Activation Keys and paste into the Activation Key fields in the License tile.

4 Settings tile

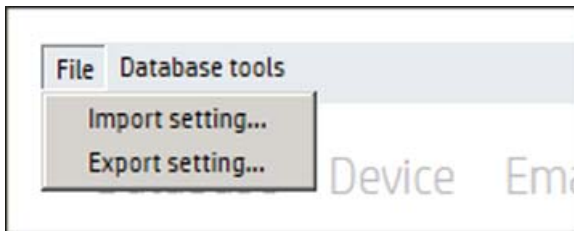
The Settings tile allows you to view and change all the settings of installed components from one location.

 **IMPORTANT:** After making changes in the Settings tile, be sure to click the corresponding **Apply** button to apply the settings.

 **NOTE:** Information in the Settings tile may vary depending on what components of HP Access Control (HP AC) are installed on the server.

Click the **File** menu to import or export setting information. Information you select and enter in the Settings tile can be exported as an XML file. It is recommended to export settings in case the server or application needs to be reinstalled.

Figure 4-1 Settings file menu



- Click **Import setting** if you want to import an XML file of previously saved settings.
- Click **Export setting** if you want to save your current settings as an XML file.

The **Database tools** menu allows you to repair or backup the database of setting information in case the server or application needs to be reinstalled. Information you select and enter in the Settings tile is stored in a database.

- Click **Compact and repair database** to compact the database file.
- Click **Backup database** to save the database as an SDF file.

4.1 Database tab

The Database tab allows you to setup or modify the connection to the SQL Server database where job accounting reports are stored.

Figure 4-2 Database tab

The screenshot shows the 'Database' tab in a configuration window. The top navigation bar includes tabs for Database, Device, Email, IIS, SPPE, Agent, Print server, and IPM. The 'Database' tab is selected. The 'Database configuration' section contains a text field for 'SQL server' with the value '(local)', two radio buttons for 'Windows authentication' (selected) and 'SQL authentication', and 'Test' and 'Apply' buttons. The 'Agent configuration' section contains a checkbox for 'LocalSystem account' (unchecked), text fields for 'Domain\User' (domain\user) and 'Password' (masked with asterisks), a checked checkbox for 'Enable IIS anonymous authentication', a checkbox for 'Restart services after update (w3svc + agent)' (unchecked), and 'Test' and 'Apply' buttons.



NOTE: The **Database** tab displays if HP Access Control (HP AC) Job Accounting is installed.

The **Database configuration** section contains the method to connect to the SQL database/instance containing job accounting data. The SQL Server field displays the name and instance of the SQL Server installed. If you are connecting to a SQL Server on a different server, make sure the name and instance of the SQL Server is correct.

There are two possible authentication methods to connect to the job accounting database stored in SQL Server: Windows authentication or SQL authentication.

- If **SQL authentication** is selected, make sure the SQL credentials in the User and Password fields are correct.
- If **Windows authentication** is selected, make sure the LocalSystem account checkbox in the Agent configuration section is unchecked. Enter the correct Windows credentials in the Domain\User and Password fields.

The **Agent configuration** section contains credential fields to allow access to the Job Accounting website. When the **LocalSystem account** checkbox is unchecked, Windows credentials must be entered in the Domain\User and Password fields. Click the **Enable IIS anonymous authentication** checkbox to assign the IIS anonymous user identity to the username entered in the Domain\User field. This allows only the domain user to access the Job Accounting website.

4.2 Device tab

The **Device** tab allows you to setup the device administrator password, setup the OPS server, select tracking options, and modify the SNMP connection to devices.

Figure 4-3 Device tab

The screenshot shows the 'Device' tab configuration interface. At the top, there are tabs for Database, Device (selected), Email, IIS, SPP Enterprise, Alias, Agent, Print server, and IPM. The 'Device' section includes fields for Administrator user name (admin), Administrator password (masked), a checkbox for 'Disable device ping', and a Certificate field (C:\Program Files\Hewlett-Packard\HP Access Control\10.96.141.172.cer) with an 'Apply' button. The 'Tracking' section has radio buttons for 'Network name' (selected) and 'Device name', with an 'Apply' button. The 'OPS server' section includes an OPS server URL (https://10.96.141.172:8081), a checkbox for 'Override OPS settings', User (admin), Password (masked), a 'Test' button, and an 'Apply' button. The 'SNMP' section includes fields for Get community name, Set community name, a dropdown for Trap level (Printer confirmation traps), Time-out (ms) (1000), SNMP retries (0), UDP port (162), and Filter delay (ms) (0), with an 'Apply' button. The 'Concurrent connections' section has a Number of connections field (20) and an 'Apply' button.

 **NOTE:** The Device tab displays if DTM, Device Analysis, Agent, or Secure Pull Print Express is installed.

Figure 4-4 Device settings

This screenshot shows a portion of the 'Device' tab configuration interface, specifically the 'Device' section. It includes fields for Administrator user name (admin), Administrator password (masked), a checkbox for 'Disable device ping', and a Certificate field (C:\Program Files\Hewlett-Packard\HP Access Control\10.96.141.172.cer) with an 'Apply' button.

In the **Device** section, the device administrator user name and password is required for communication between the server and devices. This is necessary to install and configure solutions on devices. Make sure the Administrator user name and password in the Device section matches the administrator user names and passwords of all the devices you want to configure.

Click the **Disable Device Ping** checkbox to not allow pinging between devices and the server, and to only perform telnet communications between devices and the server. By default, ping is used to detect the presence of a device IP, then telnet is used to verify that the device is a printer. Select this checkbox if ping is disabled in your network, so that only telnet will be used.

The Certificate field displays the OPS certificate required to configure pull printing on HP Officejet Pro printers. HP OXPd Professional Services (OPS) brings OXPd functionality to HP Officejet Pro devices by hosting all printer configurations. The OPS certificate is created to establish secure communication between the server and Officejet Pro printers.

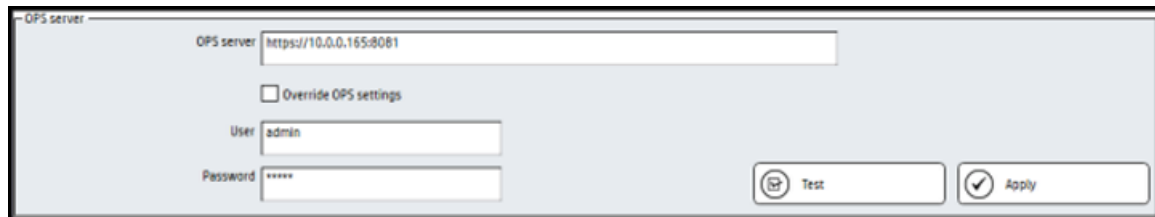
Figure 4-5 Tracking settings



In the **Tracking** section, select what device information you want to display in job accounting reports when HP FutureSmart devices are configured for tracking.

- Select **Device name** to display the device names in job accounting reports.
- Select **Network name** to display the host names of devices in job accounting reports. Make sure the **Get community name** is entered in the SNMP section to be able to read the network/host names of devices.

Figure 4-6 OPS server settings



With the OPS Server, you can configure HP Officejet Pro single-function and multi-function devices for authentication and pull printing. When Agent or Secure Pull Print Express is installed on the server, the OPS Server is installed and started. For more information about configuring HP Officejet Pro devices, see the *HP Access Control (HP AC) Secure Pull Print Express Admin Guide*.

In the **OPS Server** section, make sure the OPS Server field displays the correct server name where OPS is installed. Also, make sure port 8081 is open for connection between the OPS Server and HP Officejet Pro devices.

Click the **Override OPS settings** if you will be configuring an Officejet Pro printer that was previously configured on a different server. This checkbox allows you to override previous configuration settings when the printer is configured on the current server.

Enter the correct **User** name and **Password** that was set up during the installation of OPS Server.

 **NOTE:** The OPS password can be changed by reinstalling OPS. The opssetup.exe installation file can be found in the **C:\Program Files\Hewlett-Packard\HP Access Control\Misc** folder.


Click **Test** to test the connection to the OPS Server and make sure port 8081 is open.

Figure 4-7 SNMP settings



In the SNMP section, set the **Get** and **Set** community names for communication to and from devices. The **Get community name** allows the server to retrieve device and tracking data from a configured device. The **Set community name** allows the server to send information to the device, such as a reboot command. By default,

the Get and Set community names are “public”. For communication between the server and devices, the Get and Set community names on the server must match the Get and Set community names on all devices.

 **NOTE:** The SNMP section displays if Job Accounting, Device Analysis, Agent, or Secure Pull Print Express is installed on the server.

In the Trap level field, select the type of traps you want to track with Direct Tracking Module (DTM). A trap is a packet of information provided by the printer that indicates basic job information and print job status.

- **Print Confirmation traps** is the default Trap level. With Print Confirmation traps selected, only printed job traps are sent from the device. This is used to reduce the network traffic with unwanted traps.
- **All traps** are to track all jobs, printed, copied, or digitally sent. Some versions of HP JetDirect require that **All traps mode** is selected.

The **UDP port** field is the port used by the trap service. By default, the trap service uses UDP port 162. If the port is used by another application or service on the same server, the Job Accounting Trap service can use another port. If the port is changed, the Job Accounting Trap service (HPACJA_SnmpTrap) needs to be stopped and restarted. Printers also need to be reconfigured using the new port.

The **Filter Delay** is used if JetDirect sends the same trap multiple times in a very short interval. This occurs on external JetDirect 300x and 500x. The delay value can be set to 50 ms for 300x and 500x. For other devices, the default value can remain at 0.

In the Concurrent connections section, set the number of network devices you want to install and configure at one time. The maximum number of concurrent connections allowed is 50.

Figure 4-8 Concurrent connections




4.3 Email tab

The **Email** tab allows you to setup email server settings to send HP Access Control (HP AC) notifications to users and to allow users to email jobs for pull printing.

Figure 4-9 Email tab


The screenshot shows the 'Email' tab in a settings application. At the top, there are tabs for 'Database', 'Device', 'Email' (selected), 'IIS', 'SPPE', 'Agent', 'Print server', and 'IPM'. The 'POP3/IMAP' section has a 'Connection' dropdown set to 'IMAP', 'Server name', 'Server port' (143), 'Login', 'Password', and 'Interval (seconds)' (30). There is an 'SSL' checkbox. The 'SMTP' section has 'Server name', 'Server port' (25), 'Login', 'Password', 'Sender e-mail address', 'Recipient e-mail addresses', 'Email subject' (HP AC Secure Pull Printing), and 'Email body' (The file [0] can't be processed). Both sections have 'Test' and 'Apply' buttons.

 **NOTE:** The Email tab displays if Job Accounting, Device Analysis, IPM, Agent, or Secure Pull Print Express is installed.

In the **POP3/IMAP** section, enter your company's email server information if you want to allow users to email jobs for pull printing. The Secure Pull Print Express email service checks for and processes emailed jobs from users.

Figure 4-10 POP3 IMAP settings

This screenshot shows a close-up of the 'POP3/IMAP' section from the previous figure. It includes the 'Connection' dropdown (set to IMAP), 'Server name', 'Server port' (143), 'Login', 'Password', and 'Interval (seconds)' (30) fields. The 'SSL' checkbox is also visible. 'Test' and 'Apply' buttons are at the bottom right.

 **NOTE:** The POP3/IMAP section displays only if Secure Pull Print Express is installed.

In the Connection field, select **POP3** or **IMAP** as the connection method to the email server.

In the **Server name** field, type the name or address of the email server you want the Secure Pull Print Express email service to check for emailed jobs from users.

The **Server port** field displays the default server port for POP3 or IMAP. The default POP3 server port is 110. The default IMAP server port is 143. Click the **SSL** checkbox if the email server requires a secure connection. If you click the SSL checkbox, the **Skip SSL validation** checkbox displays. Click **Skip SSL validation** to allow the service to connect to the email server via SSL without installing a valid certificate on the server.

In the **Login** and **Password** fields, type the login name and password for access to the email server.

In the **Interval (seconds)** field, you can change how often the Secure Pull Print Express email services checks for emails. The default time is 30 seconds.

Figure 4-11 SMTP settings

The screenshot shows a configuration window titled "SMTP". It contains the following fields and controls:

- Server name:** An empty text input field.
- Server port:** A text input field containing "25". To its right is a checkbox labeled "TLS".
- Login:** An empty text input field.
- Password:** An empty text input field.
- Sender e-mail address:** An empty text input field.
- Recipient e-mail addresses:** An empty text input field.
- Email subject:** A text input field containing "HP AC Secure Pull Printing".
- Email body:** A text input field containing "The file {0} can't be processed".
- Buttons:** At the bottom right, there are two buttons: "Test" (with a document icon) and "Apply" (with a checkmark icon).

The **SMTP** section allows you to configure emails you want to send from the server. The following information can be emailed:

- Job Accounting reports
- Results of Device Analysis scheduled scans
- IPM notifications via the Email rule
- Secure Pull Print Express or Secure Pull Print Enterprise notification if a user's job cannot be processed
- AD User Editor information, AD Group Manager information, and User List Editor PINs

In the **Server name** field, type the name or address of your company email server.

In the **Server port** field, type the email server port. The default port is 25. Click the **TLS** checkbox to enable the Transport Layer Security protocol to encrypt and deliver mail securely.

In the **Login** and **Password** fields, type the login name and password for access to the email server.

In the **Sender email address** field, type the email address you want to appear in the "From" field of emails. For Secure Pull Print Express purposes, it is recommended to use the same email address that users email jobs to, so that users receive notification emails from the same address they emailed.

In the **Recipient email addresses** field, type email addresses to test the connection between the email server and recipient email addresses. This determines if a recipient can receive an email from the email server. Click the **Test** button to send an email to the recipients. A popup window appears to display information about the connection.

In the **Email subject** field, type the subject of the notification email. If Secure Pull Print Express is installed, the default email subject is "HP AC Secure Pull Printing".

In the **Email body** field, type what you want to appear in the body of the notification email. If Secure Pull Print Express is installed, the default is "The file {0} can't be processed", where {0} represents the name of the job.

4.4 IIS tab

The IIS tab contains IIS and web service settings.

Figure 4-12 IIS tab

Server name	IP	Description	Status
WB2008.tech.com	10.96.140.12		Ok
WB2003.tech.com	10.96.140.70		Ok
HPAC-VS1.support.com	10.96.141.73		Ok
*			

☐ Encrypt all web communication (devices)

☐ Use server name instead of IP (devices)

Test Apply

Agent license service

IP address: 10.96.140.12 Apply

Push mode

HTTP/FTP: http Port: 80 Login:


 **NOTE:** The IIS tab displays if Job Accounting, Agent, IPM, Secure Pull Print, Secure Pull Print Enterprise, or Secure Pull Print Express is installed.

Figure 4-13 Web service settings

Server name	IP	Description	Status
WB2008.tech.com	10.96.140.12		Ok
WB2003.tech.com	10.96.140.70		Ok
HPAC-VS1.support.com	10.96.141.73		Ok
*			

☐ Encrypt all web communication (devices)

☐ Use server name instead of IP (devices)

Test Apply

The Web service is used for the following:

- For multi-function devices to communicate with the Job Accounting website to determine quotas for copies and digital sending jobs
- To send IPM notifications to client desktops
- For users to access Pull Printing jobs from a printer, mobile device or web page
- For the server to communicate with the IRM license website
- For central management of printer fleets. When multiple servers are entered in the Web service settings and when devices are configured in the Devices tile, a dropdown list displays in the Configure window, allowing you to select the server you want to configure the device to. From one central server, you can configure printers to be managed by a different server.

The **Server name** and **Server IP** fields display the name and IP address of the server containing the Quota, IPM, and Pull Printing web services. Make sure the information is correct to allow for communication between the web service and client desktops or devices. To add additional servers, enter the Fully Qualified Domain Name (FQDN) of the additional server in the **Server name** column and enter the IP address of the server in the

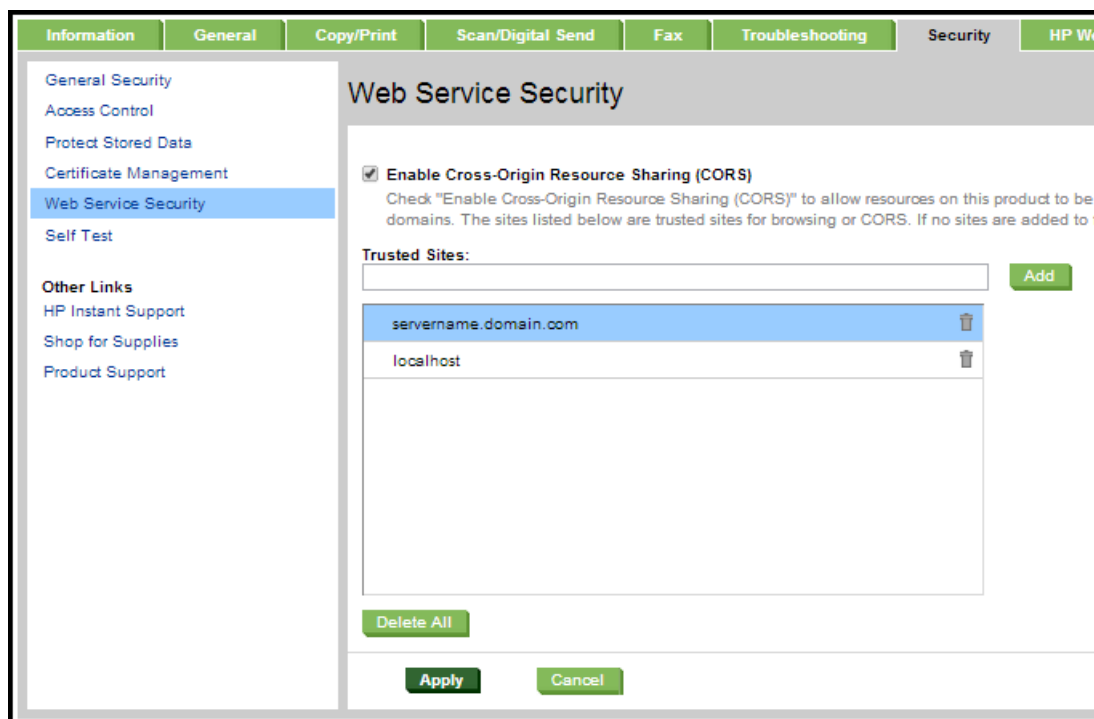
IP column. Click the **Test** button to test the connection. The Status column should display OK. Then click **Apply**.


Click the **Encrypt all web communication (devices)** checkbox if you want to enable the HTTPS protocol for communications between devices and the server.

Click the **Use server name instead of IP (devices)** checkbox for one or both of the following reasons:

- If the server name was entered during the installation and configuration of the OPS server. See the *HP Access Control (HP AC) Install Guide* for more information about the installation of the OPS server.
- If the web service security feature Cross-Origin Resource Sharing (CORS) is enabled on FutureSmart devices. To pull print at the device with Secure Pull Print Express, make sure the server name is added to the CORS Trusted Sites list. To use tracking at the device with Job Accounting, make sure the server name is listed in the CORS Trusted Sites list. To pull print at the device with Secure Pull Print, make sure "localhost" is listed in the CORS Trusted Sites list.

Figure 4-14 CORS trusted sites



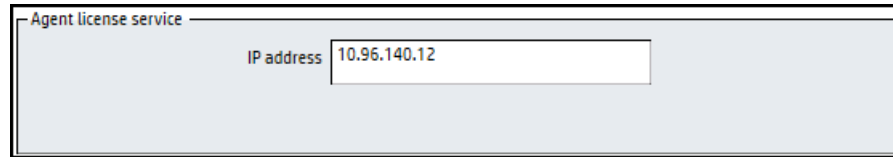
 **NOTE:** If OPS is configured on the server and you want to change the configuration of OPS to use the server name or the server IP address, follow the steps below:

1. Close the HP Access Control (HP AC) configuration tool.
2. Navigate to the **C:\Program Files (x86)\Hewlett-Packard\OPS\config** folder and open the **ops.cfg** file in a text editor application. After "host=", enter the server IP address or *servername.domain.com*, where *servername* is the name of the server, and *domain* is the name of the domain. Save and close the file.
3. Navigate to the **C:\Program Files\Hewlett-Packard\HP Access Control** folder and delete the OPS certificate file.
4. Go to **Administrative Tools > Services** and restart the OPS service. Restarting the OPS service creates a new OPS certificate using the server name or server IP address.
5. Open the HP Access Control (HP AC) configuration tool. Go to the **Settings** tile > **Device** tab and verify that the OPS certificate file name and the OPS server field contain the server name or server IP address.

Click **Test** to test the connection to the web service.

The **Agent license service** section allows you to assign a different server to handle licensing for IRM. This must be done before devices are configured. Enter the IP address of the server to handle licensing for IRM. By default, the field is populated with the IP address of the current server. After making any changes, click **Apply**.

Figure 4-15 Agent license service settings

A screenshot of the 'Agent license service' configuration panel. It features a single text input field labeled 'IP address' containing the value '10.96.140.12'. The panel has a light blue background and a dark border.

In the **Push mode** section, select a transfer protocol to auto-upload, or push, IPA tracking data from configured devices to the job accounting server.

Figure 4-16 Push mode

A screenshot of the 'Push mode' configuration panel. It includes a dropdown menu for 'HTTP/FTP' set to 'http', a 'Port' field with '80', 'Login' and 'Password' text fields, and an 'Interval (minutes)' field with '0'. At the bottom right are 'Test' and 'Apply' buttons. The panel has a light blue background and a dark border.

NOTE: The Push mode section displays if Agent or the standalone Job Accounting Print Server is installed.

In the HTTP/FTP field, select one of the transfer protocols:

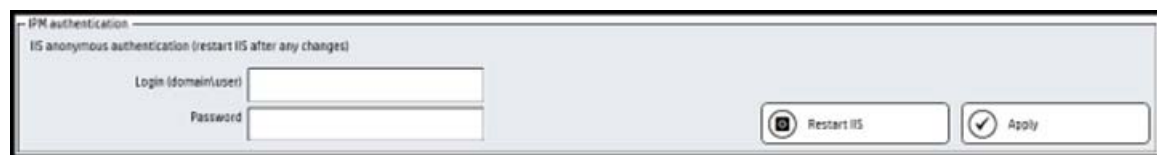
- **Hypertext Transfer Protocol (HTTP)** connections are usually terminated after a particular request has been completed. If HTTP is selected, Windows credentials are required in the Login and Password fields. Also, if IIS 7 or newer is installed on the server, Basic Authentication needs to be enabled. Devices require Basic Authentication to pass data via HTTP when IPA sends tracking data to the Job Accounting Print Server. The default port is 80.
- **File Transfer Protocol (FTP)** is best for uploading data to an internal database server. If FTP is selected, any credentials can be used in the Login and Password fields. By default, the login and password are "Anonymous". The default port is 21. Select the PASV checkbox to enable passive mode FTP if you want to allow data to transfer more easily through firewalls.

The **Interval (minutes)** field determines how often tracking data is pushed from devices to the job accounting server.

Click **Test** to test the HTTP or FTP connection.

The **IPM authentication** section contains credential fields to allow access to the IPM web service to retrieve user grouping information (user grouping is setup in the Settings tile > IPM tab > User grouping section). Windows credentials must be entered in the Login and Password fields.

Figure 4-17 IPM authentication

A screenshot of the 'IPM authentication' configuration panel. It includes a note 'IIS anonymous authentication (restart IIS after any changes)', 'Login (domain\user)' and 'Password' text fields, and 'Restart IIS' and 'Apply' buttons at the bottom right. The panel has a light blue background and a dark border.

IIS anonymous authentication means the IIS anonymous user identity will be assigned to the user name entered in the Login field. This allows only the domain user to access the IPM web service. Click **Apply**, then click **Restart IIS** to clear previous user grouping cache information.

4.5 SPPE tab

The SPPE tab contains settings for the Secure Pull Print Express component.

Figure 4-18 SPPE settings

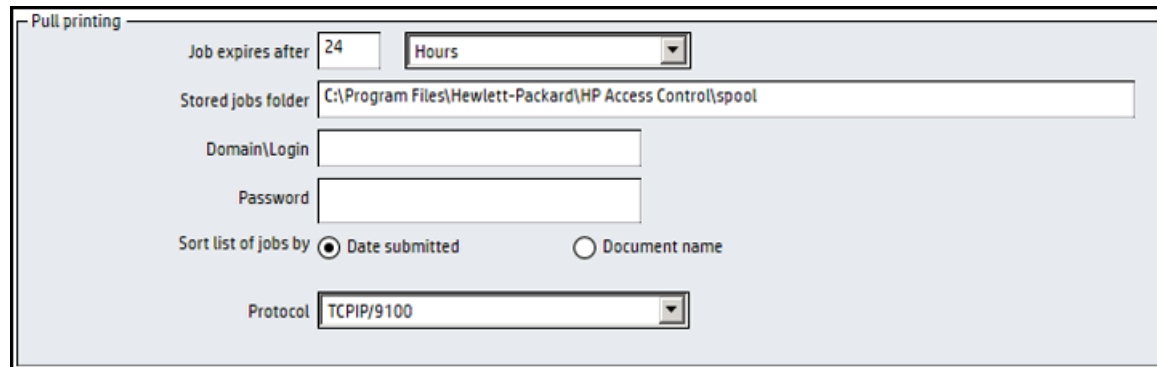
The screenshot shows the 'SPPE' tab selected in a navigation bar at the top, which also includes 'Database', 'Device', 'Email', 'IIS', 'Agent', 'Print server', and 'IPM'. The main content area is divided into three sections: 'Pull printing', 'QR code', and 'Job accounting'. The 'Pull printing' section contains fields for 'Job expires after' (set to 24) and a unit dropdown (set to Hours), a 'Stored jobs folder' text box (containing 'C:\Program Files\Hewlett-Packard\HP Access Control\spool'), 'Domain\Login' and 'Password' text boxes, a 'Sort list of jobs by' section with radio buttons for 'Date submitted' (selected) and 'Document name', and a 'Protocol' dropdown (set to 'TCPIP/9100'). The 'QR code' section has three checkboxes: 'Network name' (checked), 'IP address' (unchecked), and 'Email address' (unchecked). The 'Email' section has a checkbox for 'Process email attachments only' (unchecked) and an empty dropdown menu. The 'Job accounting' section has a checkbox for 'Enable tracking of purged jobs' (checked).

 **NOTE:** The SPPE tab displays if Secure Pull Print Express is installed.

The **Clear cache** button deletes cached information linking a user's login with the user's email address. When a user logs in at a device, information is retrieved from Active Directory, including the user's email address. The user name and email address are then stored in the cache to gather the user's printed jobs and emailed jobs under one user folder.

In the **Pull Printing** section, change the settings of stored jobs.

Figure 4-19 Pull Printing settings



In the **Job expires after** fields, select when you want jobs to expire. This can be used to manage the amount of stored jobs on the server to reduce job storage space. The default expiration time is 24 hours.

The **Stored jobs** folder field displays the default location for stored pull print jobs. Double-click the text field to browse to a different folder location. If you want to store jobs in a different folder on the network, you must have write access to the folder. In the **Domain\Login** and **Password** fields, type the credentials that have write access to the network folder.



IMPORTANT: To pull print using a shared network folder, the same service account credentials entered in the Domain\Login field must be used for read/write access to the network folder, for the HPACSPPE application pool identity, and for the Log On setting in the HP AC SPPE service.

Next to **Sort list of jobs by**, select **Date submitted** or **Document name** to determine the sort setting. The sort setting applies to the jobs list viewed on a mobile device, at a multi-function printer front panel, and on the SPPE web page.

In the **Protocol** field, select the way SPP Express will communicate with the printer. The choice of protocol will depend on the destination device, its capabilities, and the level of control and feedback required from the device.

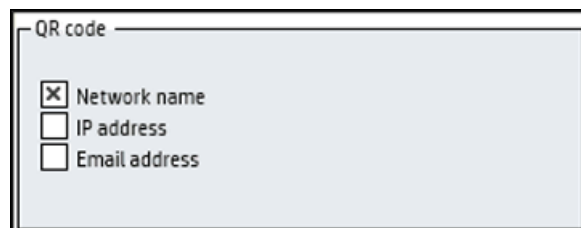
TCPIP/9100 is a direct protocol that provides a simple direct communication channel between SPP Express and the printer engine. A connection is established to TCP/IP port 9100 and all data sent by SPP Express is passed through directly to the printer.

TCPIP/LPR provides very limited feedback from devices about the success of a print request and provides no facilities for checkpoint restart of a failed request.


TCPIP/IPPS is a secure protocol that allows SPP Express to encrypt the data stream sent to the device.

In the **QR code** section, select the printer information to encode in the QR code. A user can scan a QR code with a mobile device to route stored jobs to a selected printer. If any parameter is selected, the QR code will display on the front panel when an MFP is configured for pull printing.

Figure 4-20 QR code



NOTE: The number of devices that can be configured with QR codes is unlimited. But the number of devices that can be used for pull printing is limited by the number of devices in the Secure Pull Print Express license.


 **TIP:** The order of printer information can be rearranged in the QR code. Drag and drop items in the list to change the order.

In the **Email** section, click the **Process email attachment only** checkbox if you want email attachments, not email bodies, to be processed as pull print jobs. This allows users to view their email attachments as pull print jobs in their stored jobs folder.

Figure 4-21 Email section




Email jobs must use the settings and features, such as color or duplex settings, of a printer before they can be processed as pull print jobs. Click the dropdown list to select an installed printer with the features you want to apply to email jobs. The printer must be a local printer with a PCL5, PCL6 or PS print driver.

 **IMPORTANT:** If the “Service not started with a domain account” message displays in the Email section, you must restart the HP AC SPPE Mail service with a domain account. To restart the service with a domain account, go to **Administrative Tools > Services**. Right-click the **HP AC SPPE Mail service**, then click **Properties**. Under the Log On tab, select **This account** and enter the credentials of a domain account. Click **OK**. Restart the **HP AC SPPE Mail** service.

In the **Job accounting** section, select the **Enable tracking of purged jobs** checkbox if you want to track expired pull print jobs in Job Accounting.

Figure 4-22 Job Accounting



When this box is checked, an XML file is created for each job that is purged. The XML file includes information such as the purged job name, the date the job was submitted, and the date the job was purged. The XML files are created in one of the following locations:


- If Job Accounting is installed on the same server as Secure Pull Print Express, the XML files are created in the following folder:

C:\Program Files\ Hewlett-Packard\HP Access Control\temporary\DTM

- If Job Accounting is installed on a different server, the XML files are created in the following folder:

C:\Program Files\Hewlett-Packard\HP Access Control\temporary

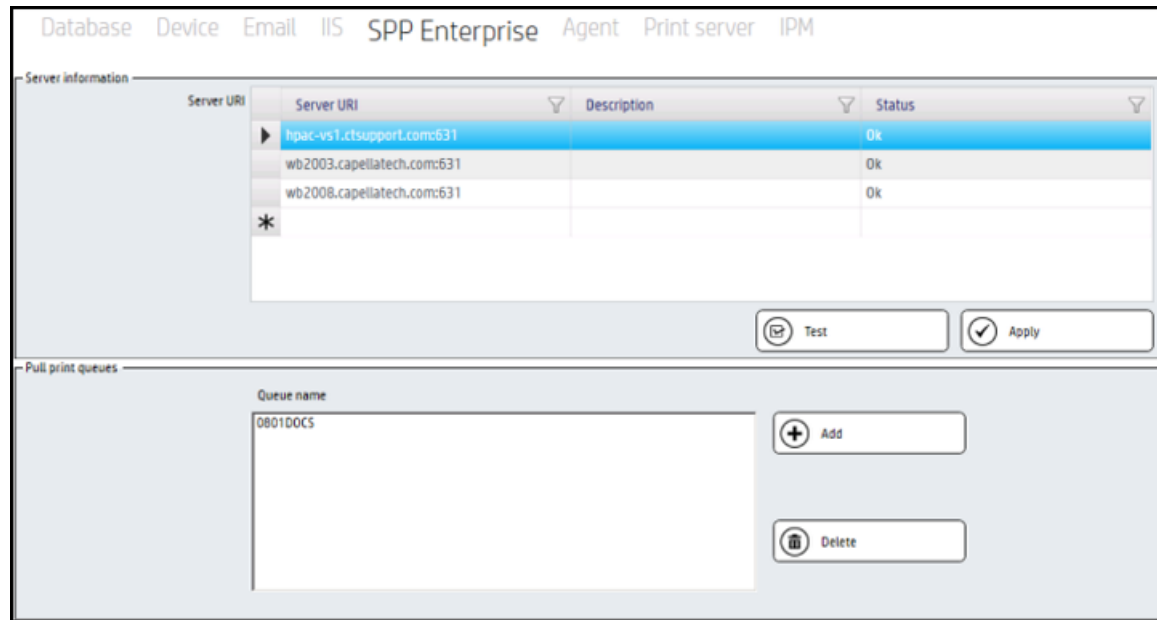
When purging is complete, the XML files are pushed to the Job Accounting server in the \Temporary \DTM folder.

 **NOTE:** If all the user’s jobs are deleted, the user’s stored jobs folder is automatically deleted.

4.6 SPP Enterprise tab

The SPP Enterprise tab contains settings for the SPP Enterprise component.

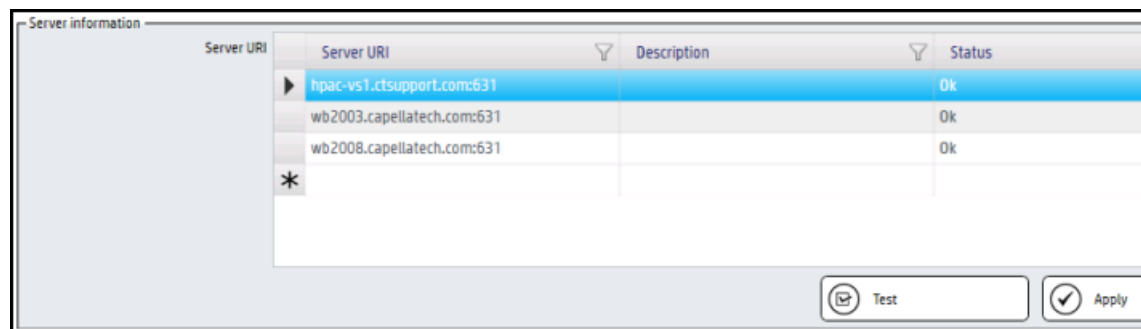
Figure 4-23 SPP Enterprise settings



NOTE: The SPP Enterprise tab displays only if the SPP Enterprise component is installed.

With SPP Enterprise users can stored jobs on one server, then release the same job at a different location from a printer configured on a different server. In the Server Information section, click an open row, then enter the Fully Qualified Domain Name (FQDN) of a server you want to add, including the IPP port number (Example: Servername.Domain.com:631). Click the Test button to test the connection to the server. The Status column should display **OK**. Then click **Apply**.

Figure 4-24 Server Information settings



If you want to store pull print jobs in a different location other than the C drive, stop the HP AC SPP Enterprise service then move the \spoolroot folder and subfolders to the new local drive. This cannot be a network share or mounted drive. Open the \bin\vpstart.ini file and enter the new location on the SERVROOT line. Save the file and restart the service after the folder has been moved.

SPP Enterprise pull print queues will allow the server to receive jobs printed from client computers. When jobs are received from client computers, the jobs are stored in the C:\Program Files\Hewlett-Packard\HP Access Control\spoolroot\spool\Queue folder, where Queue is the name of the pull print queue. Each job is stored as two files, a DAT file and an INF file. In the Pull Print Queues section, click **Add**. In the Queue name field, type any name for the pull print queue. Click **Add**.



NOTE: When a pull print queue is created from the HP AC configuration utility, a printer definition file is created in the C:\Program Files\Hewlett-Packard\HP Access Control\spoolroot\prtr folder. This printer definition file is required to allow the print queue to receive print jobs from client printers.

Figure 4-25 Pull print queues settings

Edit the following settings in the **Options** section:

- **Protocol:** This defines the way SPP Enterprise will communicate with the printer. The choice of protocol will depend on the destination device, its capabilities, and the level of control and feedback required from the device.

TCP/IP/SOCK is a direct socket protocol that provides a simple direct communication channel between SPP Enterprise and the printer engine. A connection is established to TCP/IP port 9100 and all data sent by SPP Enterprise is passed through directly to the printer.

TCP/IP/PJL implements a bi-directional communication channel with the printer engine using the PJL (Printer Job Language) job management language. This protocol provides the most sophisticated control of print delivery, including guaranteed delivery of each page to the output hopper, checkpoint restart in the event of a failure, and full device status information (i.e., page jam, load paper, etc.). The default implementation delivers one document at a time and waits for all pages to be delivered to the output tray before commencing delivery of the next document. While this provides the highest level of assured delivery, it can introduce a delay between documents caused by the printer engine winding down while the paper path is completely cleared. When printing a large number of small document this delay between jobs is most noticeable.

TCP/IP/IPPS is a secure protocol that allows SPP Enterprise to encrypt the data stream sent to the device.

- **Job expires after:** This is the expiration time for stored jobs. The default time is 24 hours. After the expiration time, jobs are deleted from the server.
- **Enable tracking of purged jobs:** When enabled, this checkbox allows expired or deleted jobs to be tracked for job accounting.
- **TCP/IP API Port:** Specifies the local TCP/IP port that SPP Enterprise will open for API requests. Port 5501 is the default port. After making any changes, make sure to click the **Restart Service** button to restart the HP AC SPP Enterprise service.
- **TCP/IP LPD Port:** Specifies the local TCP/IP port that SPP Enterprise will open for inbound LPD requests. Port 515 is the default port. If an LPD daemon is already running on the server, shut down this process to enable SPP Enterprise to open port 515. After making any changes, make sure to click the **Restart Service** button to restart the HP AC SPP Enterprise service.
- **TCP/IP IPP Port:** Specifies the local TCP/IP port that SPP Enterprise will open for inbound IPP requests. Port 631 is the default port. After making any changes, make sure to click the **Restart Service** button to restart the HP AC SPP Enterprise service.


- **Use device IP address:** When enabled, this checkbox allows the spooler to identify the printer via IP address instead of host name, in case the host name has changed and a printer has not been reconfigured. It is recommended that printers have fixed IP addresses.
- **Show local and remote jobs:** When enabled, this checkbox allows for pull print queues from all SPP Enterprise servers to automatically display on a device front panel after authentication. If this is disabled, the user will need to manually select the Remote Jobs button at the front panel to view all pull print queues.
- **QR Code:** Enable this checkbox if you want a QR code to display on the front panel of MFPs. This allows users that have the HP Mobile Release app to identify the printer for mobile pull printing.

Figure 4-26 Options

Edit the following settings in the **Email** section:

- **Process email attachments only:** Enable this checkbox if you want email attachments, not email bodies, to be processed as pull print jobs. This allows users to view their email attachments as pull print jobs in their stored jobs folder.
- **Printer dropdown menu:** This must be a pull print queue created locally on the server. This must use the settings and features, such as color duplex settings, of a printer before they can be processed as pull print jobs. Click the dropdown list to select an installed pull print queue with the features you want to apply to email jobs. The printer must be a local printer with a PCL5, PCL6 or PS print driver.

Figure 4-27 Email settings

 **NOTE:** If the “Service not started with a domain account” message displays in the Email section, you must restart the HP AC SPP Mail service with a domain account. To restart the service with a domain account, go to **Administrative Tools > Services**. Right-click the **HP AC SPP Mail** service, then click **Properties**. Under the Log On tab, select **This account** and enter the credentials of a domain account. Click **OK**. Restart the **HP AC SPP Mail** service.

4.7 Alias tab

If users do not have the same user login on all systems, aliases allow users to get their documents into the same account from all systems.

In the **Alias** tab, select a user from the list, then click **Add**.


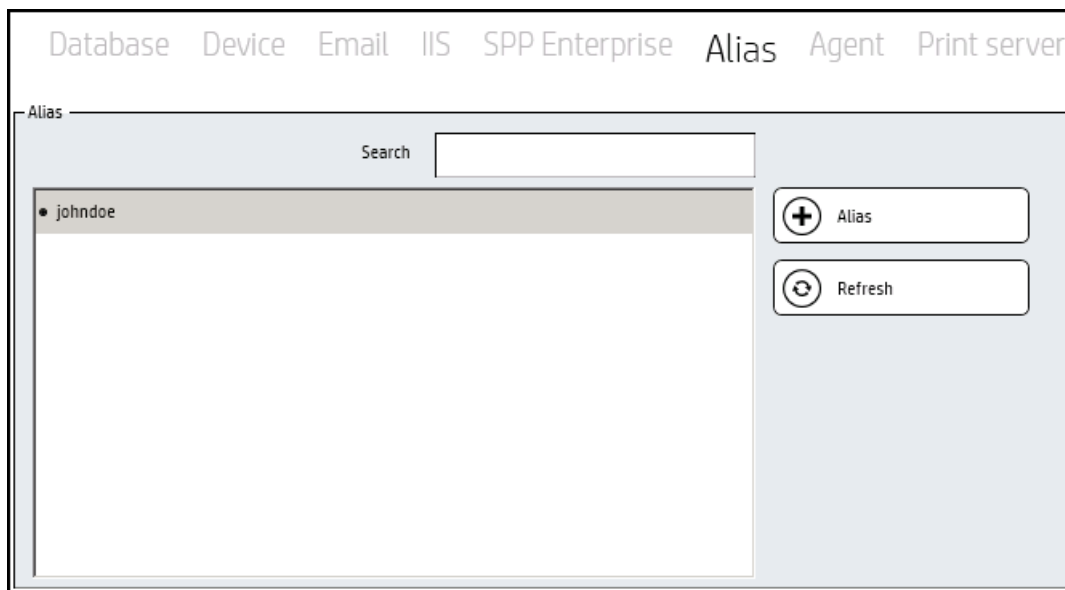
 **NOTE:** A black dot next to the user's name indicates that the user has an alias.

Figure 4-28 Alias tab




In the **Alias** text field, add an alias name. Then click **Add**. The alias must be unique in regards to other user aliases and user logons. Any number of aliases can be entered.

Figure 4-29 Alias window

4.8 Agent tab

Figure 4-30 Agent tab

 **NOTE:** The Agent tab displays if Agent is installed.

In the **HP installation files** section, make sure the correct Installation and Uninstallation PRN files display. Double-click the text field to browse to a different location.

Figure 4-31 HP install files

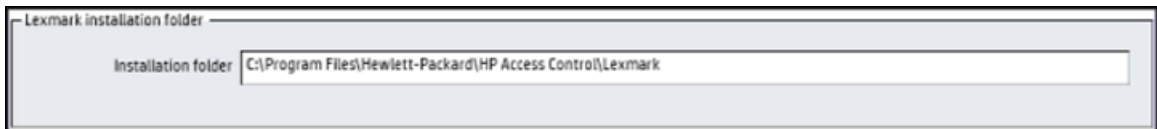


The screenshot shows a window titled "HP installation files". It contains two text input fields. The first field, labeled "Installation file", contains the path "C:\Program Files\Hewlett-Packard\HP Access Control\Firmware\HPAC-SPPE-Agent-20130731-Bundle-0-install.prn". The second field, labeled "Uninstallation file", contains the path "C:\Program Files\Hewlett-Packard\HP Access Control\Firmware\HPAC-SPPE-Agent-20130731-Bundle-0-remove.prn".

Use the Devices tile to install or uninstall the SPPE-Agent solution in HP printers.

The **Lexmark installation folder** section displays the default folder location of Lexmark installation files. Double-click in the text field to browse to a different location.

Figure 4-32 Lexmark install



The screenshot shows a window titled "Lexmark installation folder". It contains a single text input field labeled "Installation folder" with the path "C:\Program Files\Hewlett-Packard\HP Access Control\Lexmark".

Use the Devices tile to install Lexmark installation files in Lexmark printers.

In the **IRM quota web service** section, select features you want to enable.

Figure 4-33 IRM quota web service



The screenshot shows a window titled "IRM quota web service". It contains two checkboxes: "Enable quota for copies" and "Skip quota control if network failure". Below these are two text input fields: "Message" and "Error message".

Click the **Enable quota for copies** checkbox to allow the IRM quota web service to count user quotas for copies. When a user uses the copy function at a multi-function device, the web service retrieves from Job Accounting the number of remaining copies allowed for the user. The web service then communicates with the device to notify the user that he or she has reached his or her quota limit.

Click the **Skip quota control if network failure** checkbox to allow users to print after the server loses connection to the IRM quota web service. If this feature is not enabled and there is a network failure, then quotas cannot be determined and all printing stops.

In the **Message** field, type a custom message to display on the front panel of the device when a user reaches his or her quota limit.

In the **Error message** field, type a custom message to display on the front panel of the device when there is a communication error with the IRM quota web service.

4.9 Print server tab

Figure 4-34 Print server tab

Database Device Email IIS SPPE Agent **Print server** IPM

Print server tracking

☒ Port monitor

☐ Print processor

Snmp tracking

☐ Track copies

☐ Track digital sending

Print server quota web service

☐ Skip quota control if network failure

☐ End user notification

Encoding

☐ Double byte encoding

Encryption

☐ Encryption

☒ Apply



NOTE: The Print Server tab displays if the Job Accounting Print Server is installed.

In the **Print server tracking** section, select the method to gather tracking data.

- **Port monitor** creates a new port monitor for printers. This is the preferred method to gather tracking data.
- **Print processor** replaces the existing print processor with the Job Accounting print processor. This method may not work with all printer drivers.

In the **Print server quota web service** section, click to enable features of the quota web service:

- Click the **Skip quota control if network failure** checkbox to allow users to print after the server loses connection to the web service. If this feature is not enabled and there is a network failure, then quotas cannot be determined and all printing stops.
- Click the **End user notification** checkbox to enable notifications on client workstations of remaining user quotas.

In the **Snmp tracking** section, click to enable features:

- Click the **Track copies** checkbox to enable tracking of copies at multi-function printers. For more information, see the *HP Access Control (HP AC) Agent Admin Guide*.
- Click the **Track digital sending** checkbox to enable tracking of digital send jobs at multi-function printers. For more information, see the *HP Access Control (HP AC) Agent Admin Guide*.

In the **Encoding** section, click the **Double byte encoding** checkbox to track print jobs with job names containing double byte characters.

In the **Encryption** section, click the Encryption checkbox to encrypt tracking data on the print server and when data is sent to the job accounting server.

4.10 IPM tab

Figure 4-35 IPM tab

The IPM tab contains the following sections:

- IPM web service:** A checkbox for "Skip rules if network failure".
- Print activity:** A checkbox for "Enable print activity log" and a text field for "Delete log after 30 day(s)".
- Desktop notification client:** Fields for "Title", radio buttons for "Named pipe" and "Direct TCP port" (selected), "Notification" (SQ101), "Opt-in/Opt-out" (SQ102), and "Machine name".
- Cost per page:** Three identical blocks for "Econmode", "Mono", and "Color" printing, each with input fields for "Simplex" and "Duplex".
- User grouping:** Radio buttons for "Job accounting cost center" and "Active Directory", a dropdown menu, a "Search DN" field (DC=tech,DC=com), a "User name" field, and a "Test" button.
- Buttons:** "Clear cache" and "Apply" buttons at the bottom right.

NOTE: The IPM tab displays if Intelligent Print Management (IPM) is installed.

Click the **Skip rules if network failure** checkbox to allow users to print after the server loses connection to the IPM web service. If this feature is not enabled and there is a network failure, then rules cannot be checked and all printing stops.

Figure 4-36 IPM web service settings

The IPM web service settings section includes:

Server name	IP	Description	Status
WB2008.tech.com	10.96.140.12		Ok
WB2003.tech.com	10.96.140.70		Ok
HPAC-VS1.support.com	10.96.141.73		Ok
*			

Below the table are two checkboxes:

- ☐ Encrypt all web communication (devices)
- ☐ Use server name instead of IP (devices)

At the bottom right are "Test" and "Apply" buttons.

Click the **Enable print activity log** checkbox to enable a list of all jobs printed with IPM rules. The Print Activity Log can be viewed in the **IPM** tile > **Print activity log** tab.

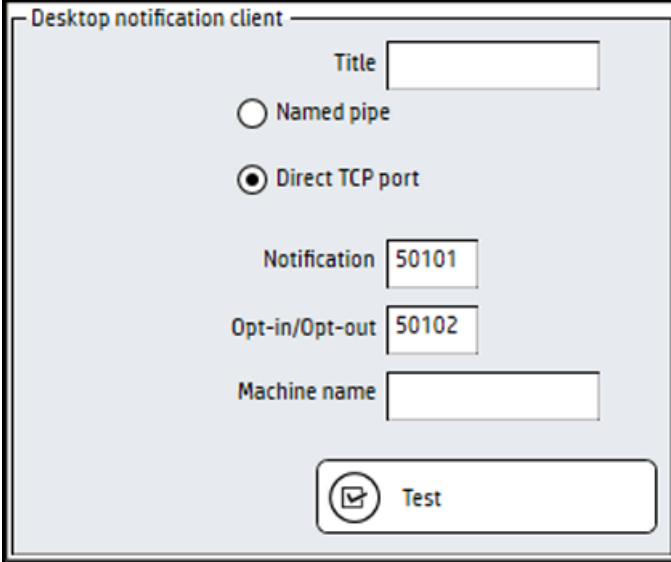
Figure 4-37 Print activity log

The Print activity log section contains:

- A checkbox for "Enable print activity log".
- A text field for "Delete log after 30 day(s)".

Enter the parameters to configure the **Notification Desktop Client**. The Notification Desktop Client is a light client application that allows notifications, such as defined printing costs, to be sent from the server to user desktops.

Figure 4-38 Notification desktop client





The screenshot shows a configuration window titled "Desktop notification client". It includes the following fields and controls:

- Title:** A text input field.
- Communication Method:** Two radio buttons. "Named pipe" is unselected, and "Direct TCP port" is selected.
- Notification:** A text input field containing the value "50101".
- Opt-in/Opt-out:** A text input field containing the value "50102".
- Machine name:** A text input field.
- Test:** A button with a checkmark icon and the text "Test".

The **Title** field displays the default title of the notification window when the window displays on client desktops. If you want to change the title of the notification window, type a new title in the Title field.

Select **Named pipe** or **Direct TCP port** as the communication method between the server and client desktops, according on your network environment.

 **NOTE:** If the TCP port is different than the default port, select **Direct TCP port**.

 **NOTE:** If the Opt-in/Opt-out rule is enabled in IPM, select **Direct TCP port**.

In the **Machine name** field, type the DNS name or IP address of a user desktop to test the connection between the server and the desktop. Click the **Test** button.

Use the cost per page feature to set estimated costs for different features within a print job. The Desktop Notification Client uses this data to notify the end user of the cost of a print job. If the Opt-in/Opt-out action is used, the user can modify the job to meet an estimated target cost.

Figure 4-39 Cost per page


The 'Cost per page' window contains three identical sections, each with a header row and three rows of input fields. Each section has a text box on the left and two columns of input fields labeled 'Simplex' and 'Duplex'.

	Simplex	Duplex
Economode	0	0
Mono	0	0
Color	0	0

	Simplex	Duplex
Economode	0	0
Mono	0	0
Color	0	0

	Simplex	Duplex
Economode	0	0
Mono	0	0
Color	0	0

Define up to three Cost per page profiles to set different cost models for different print queues.

 **TIP:** Values for duplex printing should always be lower than those for simplex printing.

The User grouping section applies when the cost center option of the IPM job stamp rule is used. When cost center is selected in the IPM job stamp rule, the name of a user's cost center group is printed on all printed pages.

Figure 4-40 User grouping

The 'User grouping' window has two radio buttons at the top: 'Job accounting cost center' (selected) and 'Active Directory'. Below them is a dropdown menu. Further down is a 'Search DN' text box containing 'DC=tech,DC=com', followed by a 'User name' text box. At the bottom is a 'Test' button with a printer icon.

The cost center information is gathered from one of the following sources:

- Select **Job accounting cost center** if you want to use cost centers defined in Job Accounting. For more information about defining Job Accounting cost centers, see the *HP Access Control (HP AC) Job Accounting User Guide*.
- Select **Active Directory** if you want to use groups defined in Active Directory. Click the dropdown list to select an Active Directory field containing the group names you want printed in job stamps.

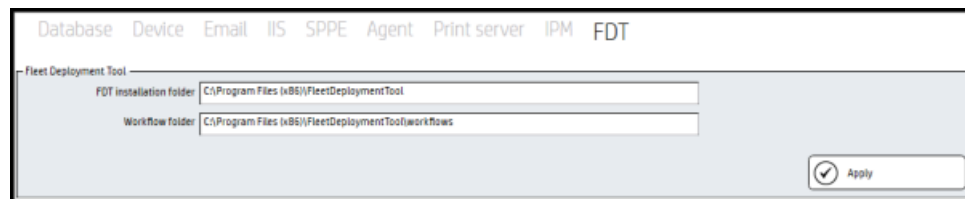
The **Search DN** field displays the domain your server belongs to.

To test the connection to Job Accounting or Active Directory, type a user name in the **User name** field, then click the **Test** button. The name of the group the user belongs to displays in the status bar at the bottom.

4.11 FDT tab

In the **FDT** tab, specify the folder containing the Fleet Deployment Tool installation folder and workflow files you want to send to devices.

Figure 4-41 FDT tab



NOTE: The FDT tab displays if the HP Fleet Deployment Tool application is installed on the server.

The HP Fleet Deployment Tool (FDT) is a standalone tool designed to install and configure your printer fleet. This FDT tab utilizes the customized workflows created by the HP Fleet Deployment Tool, allowing you to send firmware, in-printer agents or configuration files to multiple devices for a more automated deployment. See the HP Fleet Deployment Tool User Guide included with the Fleet Deployment Tool application for instructions to create workflows.

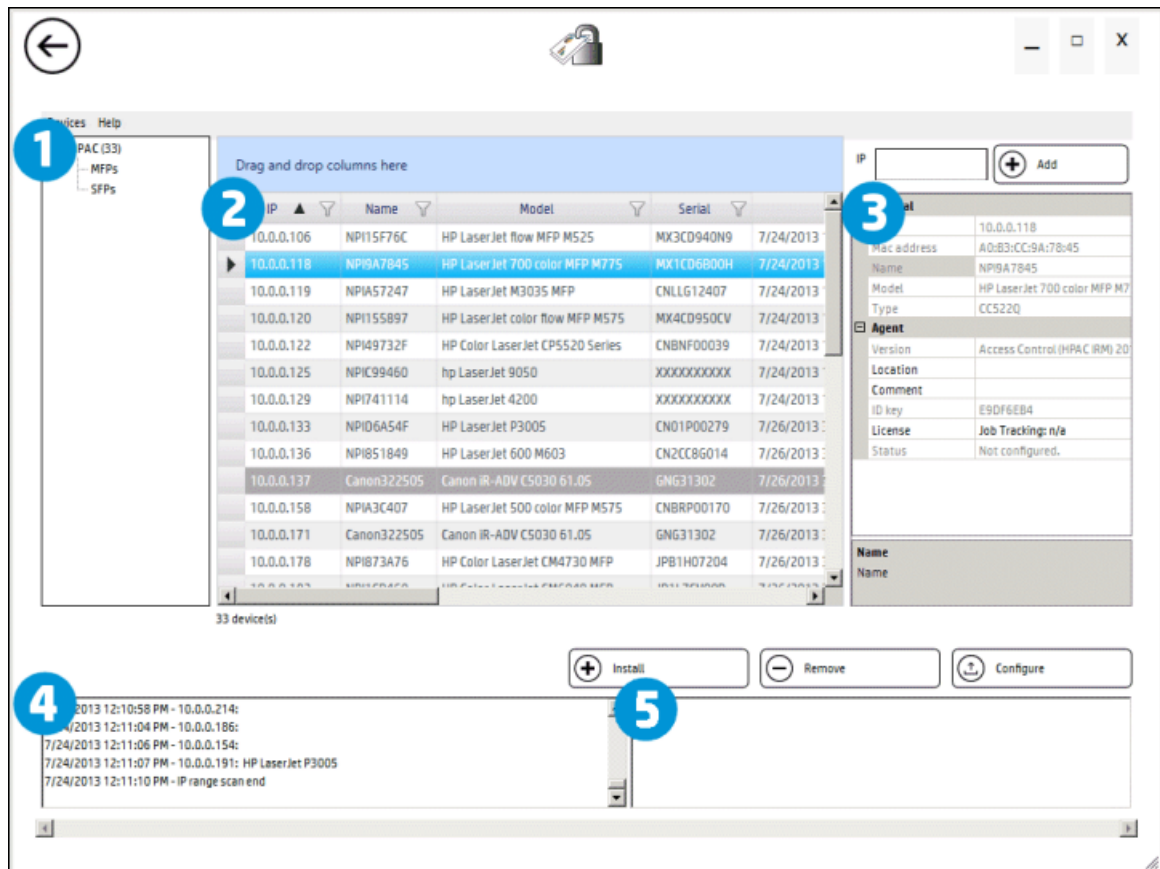
Double-click the **FDT installation** folder field to browse to the FleetDeploymentTool folder containing the FDTCommandLine.exe file.

Double-click in the **Workflow folder** field to browse to the folder containing FDT workflow files. A specific FDT workflow file is selected during the configuration of devices from the Devices tile.

5 Devices tile

The Devices tile allows you to manage devices in your printing environment. Organize devices into groups and see what is installed on each printer. From the Devices tile, you can easily install and configure printers for tracking, quota, pull printing, authentication or rights managements.

Figure 5-1 Devices tile



- 1. Device groups:** In the device groups section you can create groups to better organize your printer environment. Right-click a group name to **Add**, **Delete**, or **Rename a group**.
- 2. Device list:** The device list section displays device information, such as the device model, IP address and configuration status. When a component is configured on a device, an X displays under the Pull Printing, Tracking, Authentication, Authorization, Quota or Trap column, depending on the component that is enabled.
- 3. Device details:** The device details section allows you to view more information about a device and the solution installed. Click the License field to view a dropdown list of components that are enabled and licensed. The Location field displays location information from a FutureSmart EWS. For a non-FutureSmart device or XT device, type information in the Location and Comment fields, hit Enter, then reconfigure the device. The device details may vary, depending on what is installed on the device.

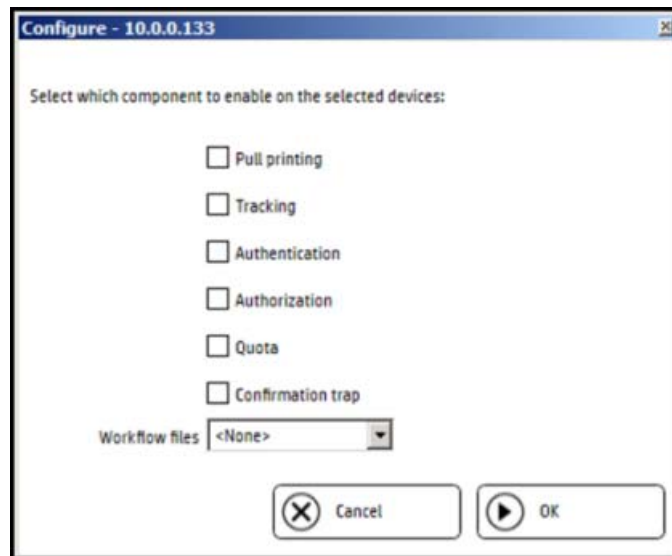
4. **Status bar:** The status bar allows you to view error messages and the status of scans or configurations. Right-click in the status bar and click Clear to delete the log information.
5. **Tracking bar:** The tracking bar displays data from devices configured for Confirmation Trap or from FutureSmart devices configured for Tracking.

Device rows in the device list may be highlighted, indicating the following:

- Yellow indicates the Agent file is installed but not configured for tracking.
- Grey indicates the device is a XT device. For more information about XT devices, see the HP AC Secure Pull Print Express Admin Guide.
- Red indicates the solution is installed but not licensed. On HP non-FutureSmart devices, red also indicates the solution is installed but not configured correctly to push tracking data to the Job Accounting server.


When you click the **Configure** button for a selected device, the Configure window displays.

Figure 5-2 Configure window



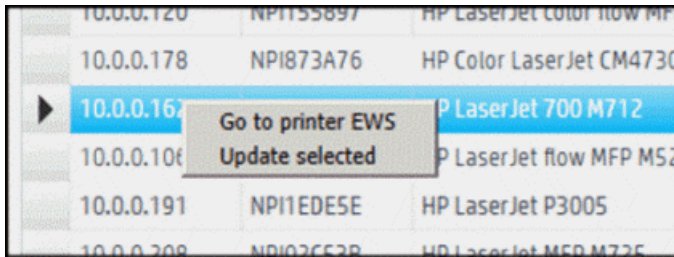
Select the components you want to enable on the selected device.


- **Pull printing:** Enable the Secure Pull Print Express button on multi-function printer front panels or enable pull printing with an XT device. The number of MFP devices that can be configured with the Secure Pull Print Express button is unlimited, but the number of devices that can be used for pull printing is limited by the number of devices in the Secure Pull Print Express license.
- **Tracking:** Enable tracking on the device. When Tracking is enabled on a FutureSmart device, information about the printer and print jobs displays in the status bar.
- **Authentication:** Enable IRM authentication on the device.
- **Authorization:** Enable IRM rights management on the device.
- **Quota:** Enable quota communication between Job Accounting and the device.
- **Confirmation trap:** Enable DTM traps on the device. When Confirmation trap is enabled on a device, information about the printer and print jobs displays in the status bar.
- **Workflow files:** Select an FDT workflow to apply on the device.

 **IMPORTANT:** Configuration at a device occurs in order, starting at the top of the Configure window list. This means the FDT workflow is always configured last on a device.

Right-click a device to display a dropdown menu of possible actions.

Figure 5-3 Devices dropdown menu



 **NOTE:** The dropdown menu options may vary, depending on the type of device and the configured components on the device.

- Click **Go to printer EWS** to go to the device's Embedded Web Server page.
- Click **Update selected** to refresh the device data.
- Click **Test trap** to test a device with the Confirmation traps component enabled.
- Click **Reboot device** to restart an XT device.
- Click **Reset to factory settings** to remove all configurations on an XT device.
- Click **Generate QR code** to create a QR code for the printer. In the QR Code window, QR code data, selected in the **Settings** tile > **SPPE** tab, displays. Print a QR code to display on single-function printers if you want users to detect the printer with the HP Mobile Release mobile app. For more information about HP Mobile Release, see the *HP Access Control (HP AC) Secure Pull Print Express Admin Guide*.
- Click **Enable OXPd 1.6 and reboot device** to enable OXPd 1.6 on HP non-FutureSmart LaserJet multi-function printers. This is to allow the HP AC Express button to display on the front panel for pull printing. If OXPd 1.6 is not enabled on the device, pull printing cannot be configured and a "OXPd 1.6 is not enabled" message displays. The Enable OXPd 1.6 and reboot device menu item displays even if OXPd 1.6 is already enabled on the device.

Figure 5-4 QR code

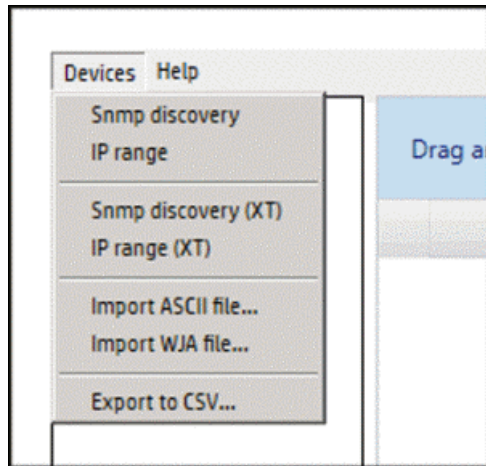


5.1 Scan the network for printers

To scan the network for single-function printers, multi-function devices, and XT devices, the following is required:

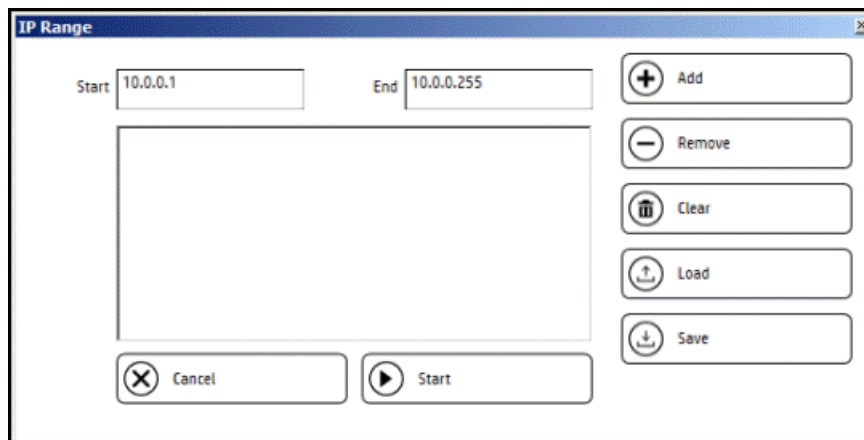
- Printers and devices must be turned on and connected to the network.
- A device administrator user name and password must be entered in the **Settings** tile > **Device** tab.

In the Devices tile, go to the **Devices** menu and select **Snmp discovery** or **IP range**.



- Snmp discovery sends a broadcast over the network and discovers available devices.
- IP range scans for devices within a selected range of IP addresses. In the IP Range window, enter IP addresses in the Start and End fields. Then click **Start** to scan the network.

Figure 5-5 IP range



TIP: To scan multiple IP ranges at once, enter an IP range in the Start and End fields, then click **Add**. Add multiple IP ranges to the list. Click **Save** to save the IP range list. Click **Load** to load a previously saved IP range list.

The progress of the scan displays in the status section at the bottom, and device data appears in the device list.

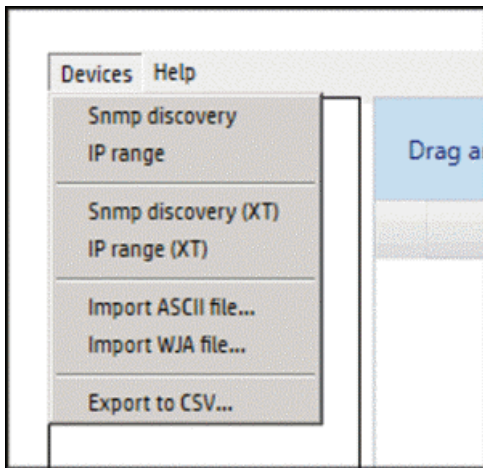
5.2 Scan the network for XT devices

The XT device is an external device with an attached card reader that allows for pull printing at any printer or multi-function device. A user simply presents his or her card at the XT card reader and all of his or her stored jobs are printed at the connected printer. For more information about XT, see the *HP Access Control (HP AC) Secure Pull Print Express Admin Guide*. To scan the network for XT devices, the following is required:

- XT devices must be connected to a power source, connected to the network, and connected to a printer.
- If your server has a firewall and you want to scan the network using Snmp discovery, make sure UDP 11000 is open.

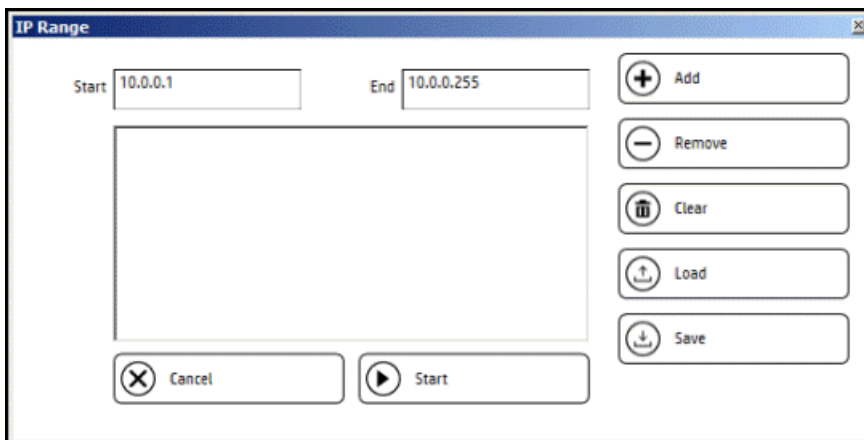
In the Devices tile, go to the Devices menu and select Snmp discovery (XT) or IP range (XT).

Figure 5-6 Devices menu



- **Snmp discovery (XT)** sends a broadcast over the network and discovers available XT devices.
- **IP range (XT)** scans for XT devices within a selected range of IP addresses. In the IP Range window, enter IP addresses in the Start and End fields. Then click **Start** to scan the network.

Figure 5-7 IP range window



The progress of the scan displays in the status section at the bottom, and device data appears in the device list.

5.3 Manually add a device

1. In the IP field, type the IP address of a device you want to add.

Figure 5-8 Add devices



2. Click **Add**.

5.4 Delete a device from the device list


1. Select the device(s) from the device list.
2. Press the **Delete** key. Then click **OK** to confirm the deletion.

5.5 Import/Export device data

To export device data to a CSV file, follow the steps below:

1. Go to the **Devices** menu and select **Export to CSV**.
2. Browse to a save location, then click **Save**.

To import a list of IP addresses/host names in ASCII format, follow the steps below:

 **IMPORTANT:** In the TXT file, each device IP address must be listed on a separate line.

1. Go to the Devices menu and select **Import ASCII file**.
2. Browse to the location of the TXT file, then click **Open**.

To import device data from a CSV file that was exported from Web Jetadmin, follow the steps below:

 **IMPORTANT:** In the CSV file, each device must be listed on a separate line.

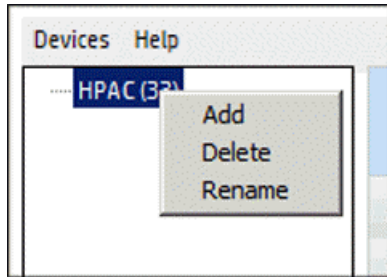
1. Go to the Devices menu and select **Import WJA file**.
2. Browse to the location of the exported CSV file, then click **Open**.

5.6 Organize and manage devices

If you want to organize devices by groups, follow the steps below:

1. Right-click the HPAC device group, then click **Add**. Give the new group a unique name.

Figure 5-9 Add device groups

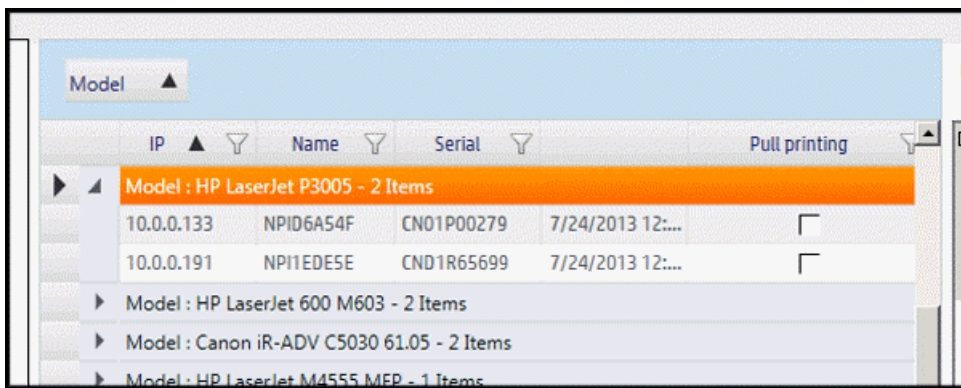


2. Click and drag devices from the device list to the new group name. This moves the device data from the HPAC group to the new group.

TIP: Create multiple groups to better organize your printer environment. For example, create a group for single-function printers named SFPs to manage the installation and configuration of only single-function printers.

If you want to better organize the information displayed in the device list, click and drag column headings to the Drag and drop columns here area.

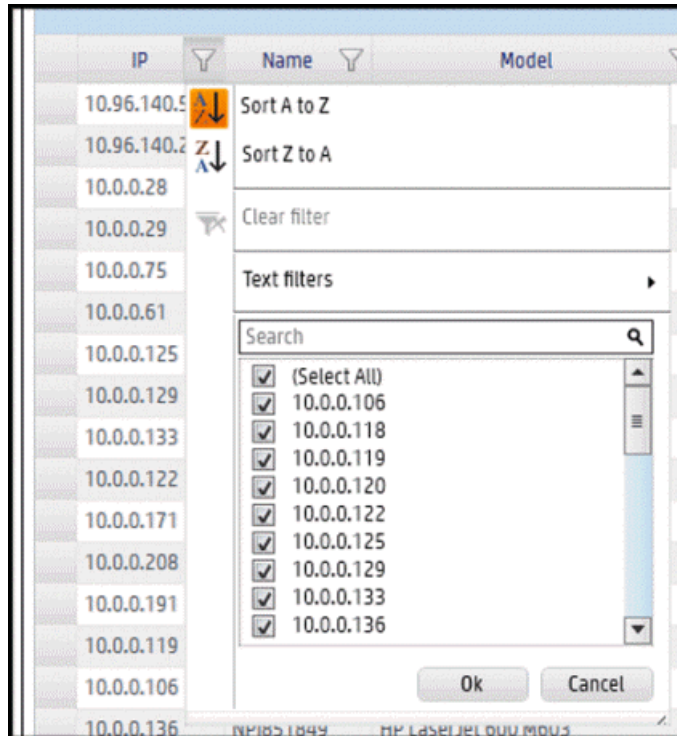
Figure 5-10 Group devices



TIP: Drag multiple columns to the drag and drop area for better organization. Rearrange the order of the columns from left to right to change the order of information displayed.

Click the filter icon in any column to sort or filter device data.

Figure 5-11 Filter devices



5.7 Install and configure components on HP FutureSmart and non-FutureSmart devices

Prerequisites:

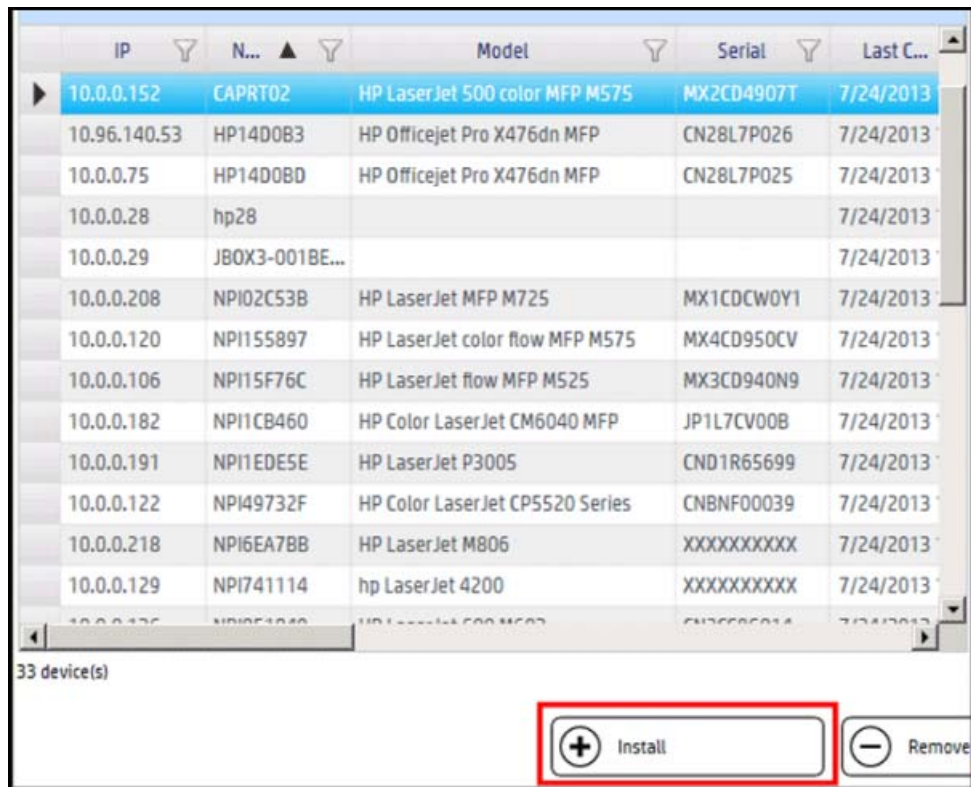
- Before installing any solution on HP devices, make sure the correct PRN installation file displays in the **Installation file** field in the **Settings** tile > **Agent** tab.
- Make sure a device administrator password is set on MFPs and matches the device administrator name and password in the **Settings** tile > **Device** tab.
- On some Non-FutureSmart MFPs, make sure to right-click the device row and select **Enable OXPd 1.6 and reboot device** before configuring the device for pull printing. OXPd 1.6 allows the pull printing button to display on the front panel.
- Make sure the printing protocol selected in the HP AC configuration tool (in the Settings tile > SPP Express or SPP Enterprise tab) is enabled on the HP device (in the device EWS > Networking tab > Other Settings page).

Follow the steps below:

1. Select the device(s) from the device list.

2. Click **Install** to send the installation file to the device(s). The HP device(s) may reboot during the installation process. Please wait for the device(s) to return to the Ready state.

Figure 5-12 Device install



The screenshot displays a table of networked HP devices. The first row is highlighted in blue. Below the table, there is a summary line '33 device(s)' and two buttons: '+ Install' and '- Remove'. The '+ Install' button is enclosed in a red rectangular box.

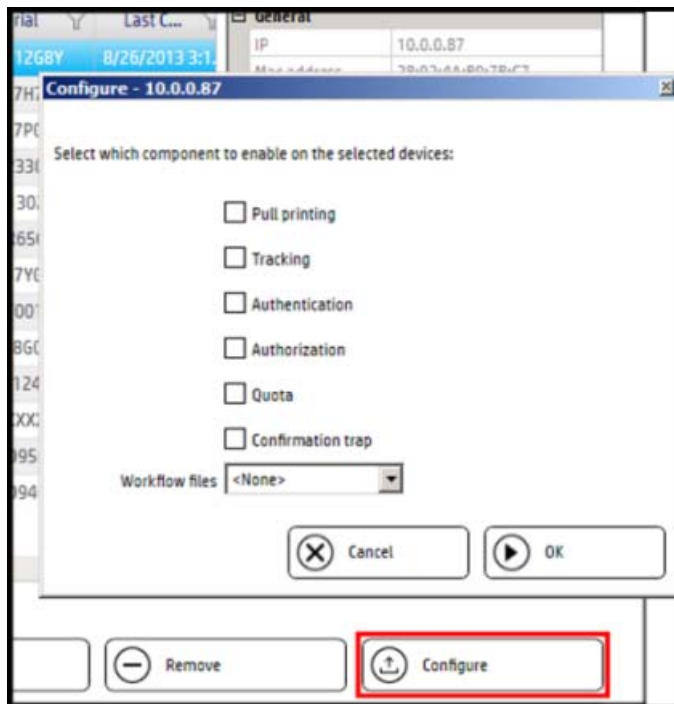
IP	N...	Model	Serial	Last C...
10.0.0.152	CAPRT02	HP LaserJet 500 color MFP M575	MX2CD4907T	7/24/2013
10.96.140.53	HP14D0B3	HP Officejet Pro X476dn MFP	CN28L7P026	7/24/2013
10.0.0.75	HP14D0BD	HP Officejet Pro X476dn MFP	CN28L7P025	7/24/2013
10.0.0.28	hp28			7/24/2013
10.0.0.29	JBOX3-001BE...			7/24/2013
10.0.0.208	NPI02C53B	HP LaserJet MFP M725	MX1CDCW0Y1	7/24/2013
10.0.0.120	NPI155897	HP LaserJet color flow MFP M575	MX4CD950CV	7/24/2013
10.0.0.106	NPI15F76C	HP LaserJet flow MFP M525	MX3CD940N9	7/24/2013
10.0.0.182	NPI1CB460	HP Color LaserJet CM6040 MFP	JP1L7CV00B	7/24/2013
10.0.0.191	NPI1EDE5E	HP LaserJet P3005	CND1R65699	7/24/2013
10.0.0.122	NPI49732F	HP Color LaserJet CP5520 Series	CNBNF00039	7/24/2013
10.0.0.218	NPI6EA7BB	HP LaserJet M806	XXXXXXXXXX	7/24/2013
10.0.0.129	NPI741114	hp LaserJet 4200	XXXXXXXXXX	7/24/2013
10.0.0.136	NPI051040	HP LaserJet 500 MFP	CN28L7P026	7/24/2013

33 device(s)

+ Install **- Remove**

3. Select the device(s) from the device list, then click **Configure**. In the Configure window, select each component you want to configure on the device(s). Click **OK**.

Figure 5-13 Configure device



IMPORTANT: When reconfiguring the device(s), place an **X** in a component checkbox to resend the configuration file. Place a **/** in a component checkbox to not resend the configuration file and leave the current configuration status as is. Clear a component checkbox to disable the component on the device.

NOTE: To remove the solution from Non-FutureSmart device, select the device from the device list, then click the **Remove** button.

5.8 Configure components on HP Officejet Pro printers

See the table below for supported HP OfficeJet Pro printers and firmware.

Table 5-1 Supported HP OfficeJet Pro printers and firmware

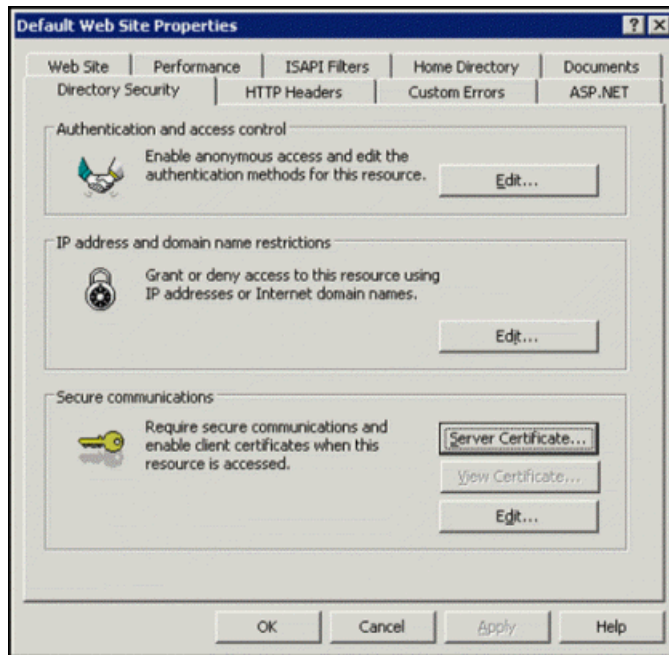
Supported HP OfficeJet Pro printer	Minimum firmware versions
HP Officejet Pro 251	EVP1CN3327DR
HP Officejet Pro 276 MFP	FRP1CN3327DR
HP Officejet Pro X476 MFP and X576 MFP	LNP1CN1327DR
HP Officejet Pro X551	BZP1CN1327DR

Before configuring an HP Officejet Pro printer from Windows Server 2003 using IIS 6, IIS 7 or newer, the SSL certificate must be manually selected in IIS. Follow the steps below:

IIS 6:

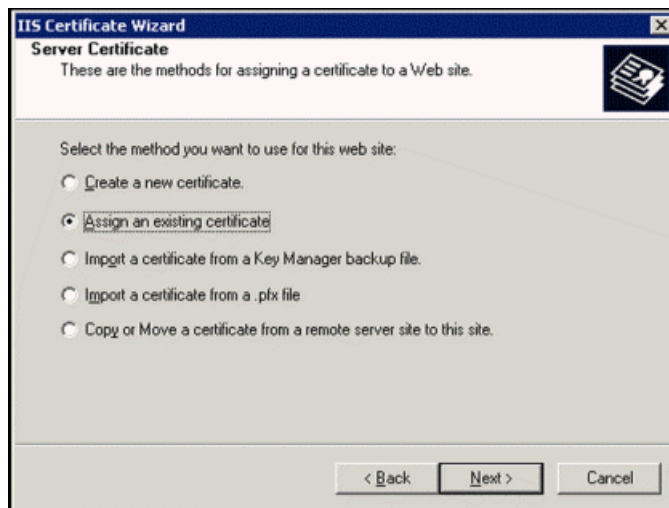
1. Go to **Administrative Tools > Internet Information Services (IIS) Manager**.
2. Select **Default Web Site** and right-click to open **Properties**.
3. In the Properties window, select the **Directory Security** tab and then click **Server Certificate**.

Figure 5-14 Default website properties



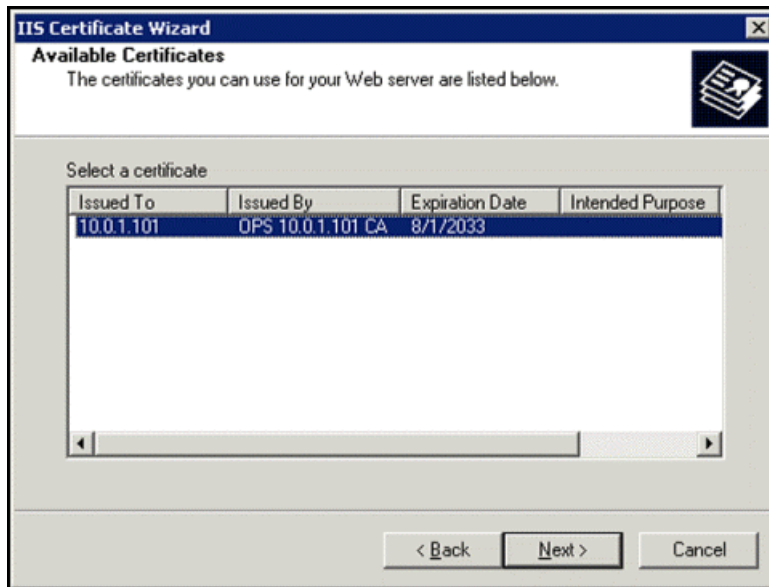
4. The Web Server Certificate Wizard opens. Select **Assign an existing certificate**. Click **Next**.

Figure 5-15 Assign an existing certificate



5. Select the OPS server certificate and click **Next**. Click **Finish** at the end.

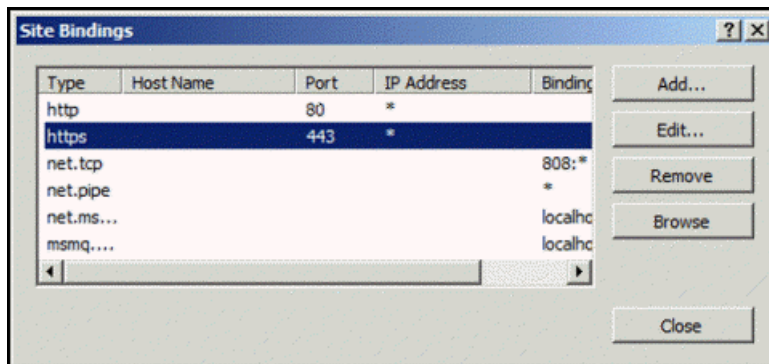
Figure 5-16 Select certificate



IIS 7 or newer:

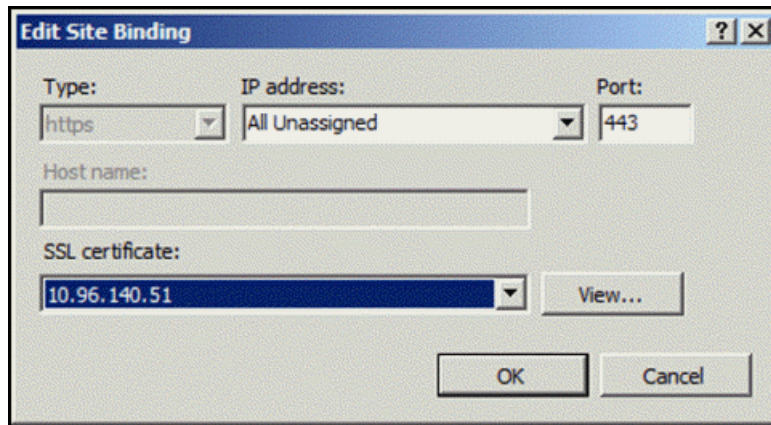
1. Go to **Administrative Tools > Internet Information Services (IIS) Manager**.
2. Select **Default Web Site** and then click **Bindings**.
3. Select **https** and then click **Edit**.

Figure 5-17 Edit bindings



4. Select the certificate from the SSL certificate dropdown menu. Click **OK**.

Figure 5-18 SSL certificate



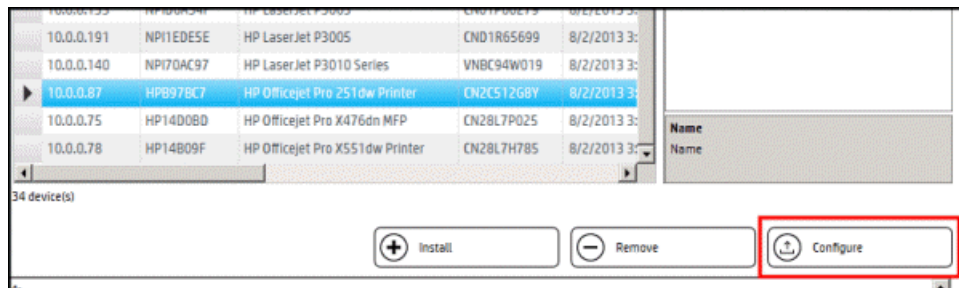
Prerequisites:

- Agent and Secure Pull Print Express must be installed on the server.
- On Windows Server 2003, make sure the OPS service is started with a domain account.
- Make sure the Officejet Pro device administrator password matches the device administrator name and password in the Settings tile > Device tab.
- Make sure the correct OPS certificate displays in the **Certificate** field in the **Settings** tile > **Device** tab.

Follow the steps below:

1. Select the device(s) from the device list, then click **Configure**.

Figure 5-19 OfficeJet configure



2. In the Configure window, select the following components:
 - Select **Pull printing** to enable the Secure Pull Print Express app button.
 - Select **Authentication** to enable IRM authentication.
 - Select **Authorization** to enable IRM rights management.
3. Click **OK**.

5.8.1 Unregister an Officejet Pro printer

If you unregister an Officejet Pro printer from the OPS server, no third party applications will work. To unregister an Officejet Pro printer from an OPS server, follow the steps below:

1. Open a command prompt and run the **OPSSetup.bat** file, located in the C:\Program Files (x86)\Hewlett-Packard\OPS\bin folder. On 64-bit servers, make sure you select "Run as administrator" when you open the command prompt.
2. From the available options, select **Unregister a device to the OPS server** and follow the on-screen instructions.

```

C:\Program Files\Hewlett-Packard\OPS\bin>OPSSetup.bat
Please select an option from below:
1. Create an instance of OPS Server
2. Create an instance of OPS Server using config file
3. Register a device to the OPS server
4. Unregister a device to the OPS server
5. Retrieve the device current OPS server details
6. Exit Setup
4

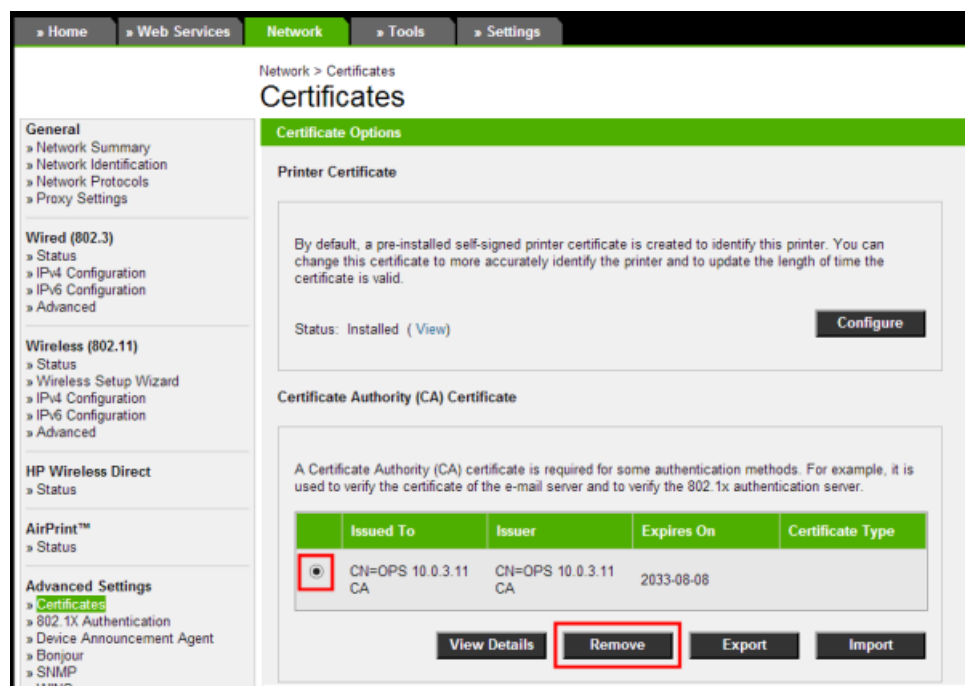
!!!Warning!!!
Unregistering the OPS might result in losing all the OXPD data in the device
Are you sure you want to unregister the OPS [default 'N']
y
Enter the device IP address
10.0.0.78
Enter the device username to be used
admin
Enter the device password to be used
admin

Details retrieved from the device
OPS Server URL = "https://10.0.3.11:8081"
OPS Server userName = "admin"

OPS Unregistered successfully
  
```

3. Open the EWS of the Officejet Pro printer and go to **Network > Certificates** page. Select the OPS certificate, then click **Remove**.

Figure 5-20 Unregister officeJet



5.9 Configure components on HP S900 series devices

Prerequisites

- Make sure PIC licenses are available on the HP AC server. A PIC license is required for each device to allow for walk-up authentication.
- If you want to use a front panel QR code for pull printing with a mobile device, make sure to manually generate a QR code prior to configuring the device.
- If you will be using SPP Enterprise on an HP S900 series device, make sure to go to the HP AC configuration tool > Devices tile and configure the device for Pull Printing. This will create a printer definition file, which is required to use SPP Enterprise. For more information, see the *HP AC SPP Enterprise Admin Guide*.

Open a web browser and enter the IP address of the device to go to the device's web page to configure the device. The default username for the device web page is "admin" and the default password is "admin".

HP S900 series devices support pull printing using SPP Express or SPP Enterprise. Follow the steps below:

1. To install a card reader for card authentication, follow the steps below:



IMPORTANT: By default, card readers are configured to read HID and iClass card types. If you want the card reader to read different card types, update the card reader before connecting to the printer. For instructions on how to configure and update the card reader, see the *Set Proximity Reader parameters* section on pages 22-25 of the *HP Access Control (HP AC) Agent Admin Guide*. Specific parts/kits along with part numbers are required for Hip reader integration on the S900 devices.

Contact your HP service tech to have a card reader installed in your S900 series device.

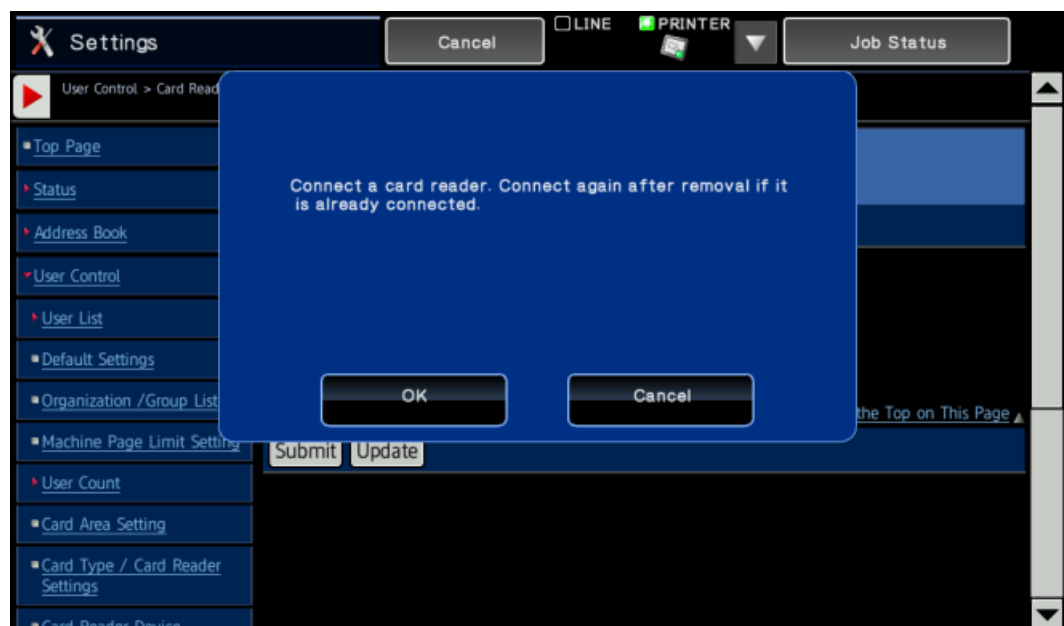
- a. Select **User Control** followed by **Card Type / Card Reader Settings**. Select the Use IC Card for Authentication checkbox. Make sure the Card Type / Card Reader value is set to 200. Click Submit(U).

Figure 5-21 Card Reader settings

The screenshot shows the HP Color MFP S962dn web interface. The top left features the HP logo and the model name. The top right shows the user name 'Administrator' and a 'Logout(L)' button. The main heading is 'Card Type / Card Reader Settings'. Below this, there are 'Submit(U)' and 'Update(R)' buttons. A dropdown menu for 'Card Type / Card Reader' is set to '200'. A checkbox labeled 'Use IC Card for Authentication' is checked and highlighted with a red box. To the right of this checkbox is a link 'Back to the Top on This Page ▲'. Below the checkbox are 'Submit(U)' and 'Update(R)' buttons. On the left side, there is a navigation menu with items: 'Top Page', 'Status', 'Address Book', 'Document Operations', 'User Control' (highlighted with a red box), 'User List', 'Default Settings', 'Organization /Group List', 'Machine Page Limit Setting', 'User Count', 'Card Area Setting', 'Card Type / Card Reader Settings' (highlighted with a red box), and 'System Settings'.

- b. At the device, tap **Settings > User Control > Card Reader Device Registration**. Then tap **Read**.
- c. When prompted, plug in the card reader. The card reader will beep twice. Tap **OK**. The card reader Product ID and Vender ID displays on the screen.

Figure 5-22 Insert card reader prompt



- d. Tap **Submit** to save the card reader registration.

Figure 5-23 Card reader registration

The screenshot shows the 'Settings' application on an HP S900 series device. The 'User Control > Card Reader Device Registration' path is selected. The left sidebar contains a list of settings categories: Top Page, Status, Address Book, User Control (selected), User List, Default Settings, Organization /Group List, Machine Page Limit Setting, User Count, Card Area Setting, Card Type / Card Reader Settings, and Card Reader Device. The main content area is titled 'Card Reader Device Registration' and displays a success message: 'Your request was successfully processed.' Below this, it says 'Register a Card Reader' and shows the following details:

Product ID	69
Vender ID	1008

Below the table are 'Read' and 'Delete' buttons. At the bottom of the main area are 'Submit' and 'Update' buttons. A 'Back to the Top on This Page' link is also present. The top of the screen features a 'Cancel' button, a 'LINE' status indicator, a 'PRINTER' status indicator, and a 'Job Status' button.

2. To configure the device for card authentication, select **User Control** followed by **Default Settings**. Scroll down to the **Card Setting** section. Select the **Automatic Login with a Card** checkbox. Select the **Card / Front Panel Operation Authentication Approved** checkbox. Specify **Enable** in the **Card ID Registration/Change Authority** dropdown.

Figure 5-24 Default settings

HP Color MFP S962dn

User Name: Administrator Logout(L)

Default Settings

Submit(U) Update(R)

User Authentication: Disable

Authentication Method Setting:

- ☒ Authenticate a User by Login Name and Password
- ☐ Authenticate a User by Login Name, Password and E-mail Address
- ☐ Authenticate a User by User Number Only

Device Account Mode Setting:

- ☐ Device Account Mode
- ☐ Allow Login by Different User

Login User: Not Set User Selection(C)

Actions when the Limit of Pages for Output Jobs:

- ☒ Job is Completed even when the Limit of Pages is Reached
- ☐ Job is Stopped when the Limit of Pages is Reached
- ☐ After reaching to the page limit, cancel the job and delete the job during receiving

☐ A Warning when Login Fails

☒ Disabling of Printing by Invalid User

☐ Automatically print stored jobs after login: Login Name

Default Network Authentication Server Setting: Not Set

☐ Perform LDAP server access control.

☒ Display Usage Status after Login

Login Name Display: Display login name

☐ Include Job Status in user authentication

☒ Automatic Logout Setting: 60 seconds

Edit Help Display of Login Screen: (Up to 256 characters)

Card Setting:

☒ Automatic Login with a Card

Authentication Method Setting:

- ☐ Only Card Authentication Approved
- ☒ Card / Front Panel Operation Authentication Approved

Card ID Registration/Change Authority: Enable

3. On the device web page, select **System Settings** followed by **Operation Settings** followed by **Home Screen Settings**.
 - a. Select the **Image** tab followed by one of the **Not Set** links.

Figure 5-25 Home screen settings

HP Color MFP S962dn

User Name: Administrator Logout(L)

Home Screen Settings

Update(R)

Item Image

Background Image Default Change(C)

No.	Name
1	Not Set
2	Not Set
3	Not Set
4	Not Set
5	Not Set
6	Not Set
7	Not Set
8	Not Set
9	Not Set
10	Not Set

Update(R) Back to the Top on This Page ▲

- b. On the **Registration** screen, specify the name of the image you wish to associate with the Top Level MFP panel for the application. The HP AC icon, named “icon48x44.png”, is located on the HP AC server in the **C:\Program Files\Hewlett-Packard\HP Access Control\DPR** folder. Click **Submit(U)**.

Figure 5-26 Home screen registration

HP Color MFP S962dn

User Name: Administrator Logout(L)

Home Screen Registration

Submit(U) Cancel(C)

File Name: Not Set

Select File: Choose File No file chosen (Up to 200 characters)

Notice: The supported file types JPEG with file extensions jpeg, jpg, jpe and jif. GIF with file extensions gif. PNG with file extensions png.

Submit(U) Cancel(C) Back to the Top on This Page ▲

- c. After adding the custom image, select the Item tab followed by the Apps Home Button link. Scroll to the bottom of the page and select the **Use Custom Image** checkbox. Then specify the image you added in step 4b. Then select **Reboot Now** to reboot the device and apply the settings.

Figure 5-27 Custom image

Security Settings

Custom Links

Operation Manual Download

Image:

☒ Use Custom Image

Select File: logo48x44.gif

Submit(U) Cancel(C) Back to the Top on This Page ▲

4. To register HP AC Express with the MFP, select **Application Settings** followed by **External Applications Settings**.

Figure 5-28 Standard Application settings

HP Color MFP S962dn

User Name: Administrator Logout(L)

Standard Application Settings

Update(R)

Application Name	No.
AC Express	1

Select All(S) Clear Checked(K)

Delete(O) Add(Y)

Update(R)

Back to the Top on This Page ▲

From the External Application Settings, select the **Add** button. Specify the Application Name as **AC Express**. Specify the Address for Application UI as **http://serverIP/HPAppsWS/Default.aspx**, where serverIP is the IP address of the server. On the same page, select the **Use Custom Icon** checkbox and then select the image you wish to associate with the Print Pulling application.

Figure 5-29 Standard Application registration

HP Color MFP S962dn

User Name: Administrator Logout(L)

Standard Application Registration

Submit(U) Cancel(C)

Standard Application Registration

Application Name: AC Express Up to 36 characters)

Address for Application UI: http://10.0.0.123/HPAppsWS/Default.aspx Up to 127 characters)

Timeout: 20 seconds(1-60)

☐ Extended Platform

☐ Use Proxy Server

Data Size: X= dot(200-2000) Y= dot(200-2000)

Display Style: ☒ Full ☐ Expand ☐ Fixed Size

☒ Use Custom Icon

File Name: logo48x44.gif

Select File: Choose File No file chosen (Up to 200 characters)

Notice: The supported file types: JPEG with file extensions .jpeg, .jpg, .jpe and .jif. GIF with file extensions .gif. PNG with file extensions .png.

Submit(U) Cancel(C)

Back to the Top on This Page ▲

5. To register the HPAuthWS authentication application with the MFP, select **Application Settings** followed by **External Applications Settings** followed by **External Accounting Application Settings**.
 - a. Select **Enable** in the **External Account Control** dropdown.
 - b. Select the **Set Authentication Server (Server 1)** checkbox.
 - c. Select **Enable** in the **Server 1** dropdown.
 - d. Specify an **Application Name**.
 - e. Specify the **Address for Application UI** as http://serverIP/HPAuthWS/Default.aspx, where serverIP is the IP address of the server.
 - f. Specify the **Address for Web Service** as http://serverIP/HPAuthWS/MFPSink.asmx, where serverIP is the IP address of the server.

Figure 5-30 External accounting application settings

- g. Click **Submit**. Then select **Reboot Now** to reboot the device and apply the settings.

5.9.1 Pull printing at the device

Prerequisites:

- On the server, open the HP AC configuration tool, go to the **IRM** tile > **AD Configurator** tab and make sure the IRM settings are correct for authentication.



NOTE: If you change the IRM authentication method to Code Only, you must recycle the HPACWS application pool before authenticating at the device. If an error message displays on the front panel, power cycle the device.

- To use card authentication, make sure a card reader is connected to the device and cards are registered to users. To enroll cards to users, use the Card Enrollment application from a desktop or use the Card Enrollment feature at an HP LaserJet MFP or HP OfficeJet Pro.
- If you chose to use the TCPIP/IPPS protocol in the HP AC configuration tool > Settings tile > SPP Express or SPP Enterprise tab, make sure IPPS-SLL is enabled on the device. Go to the device web page > **Security Settings** > **SLL Settings**. In the **Setting of SLL** section, make sure IPP-SLL is set to **Enable**. Click **Submit**.

- If the HP AC server is using IIS 6, SSL must be disabled. Go to the IIS Manager > local computer > Web Sites > Default Web site. Right-click **HPAppsWS** and select **Properties**. In the ASP.NET tab, click **Edit Configuration**. In the General tab, set the UseSSL application setting to **false**. Click **OK**. Make the same change to the HPAuthWS web site.
- If you will be using SPP Enterprise, make sure the device is configured for Pull Printing.

Follow the steps below to release stored jobs at the device:

1. To login at the device, present your card at the card reader or enter your PIC to authenticate.
2. Touch **Apps**. If more than one application is configured on the device, tap the pull printing application.

Figure 5-31 Apps



3. Select documents from the document list. Tap **Print All** to print all documents in the list. Tap **Print-Delete** to print and then delete the document from the document list. Tap **Print-Keep** to print and keep the document in the document list.

TIP: If a user is logged in and another user presents his proximity card at the card reader, the first user will be automatically logged out and the second user will be logged in.

NOTE: If the IRM authentication method is set to Card + Code (dual factor) and you log out by presenting a proximity card at the card reader, the following message displays: "Authentication failed. Please confirm the card." Tap **OK** to log out.

5.10 Install and configure components on Lexmark devices

Before the HP Access Control (HP AC) applications can be used on the Lexmark MFP front panel, MFP devices must have the HP Access Control (HP AC) Lexmark Applications solution installed and enabled. This Lexmark eSF (Embedded Solutions Framework) solution allows HP Access Control (HP AC) applications to be server-based, giving the Lexmark MFP the ability to display the menus and communicate with the jobs folder on the HP Access Control (HP AC) servers, without having any components residing directly on the MFP.

See the table below to determine which printers are supported.

Model	eSF Version
651de, X652de, XS651, XS652	2.1

X654de, X656de, XS654, XS656	
X658de, XS658	
X738de, X736de, X734de, X738dte, XS734, XS736, XS738	
X466dwe, X466dte, X466de, X464de, X463de*, XS463*, XS464, XS466	
T654, TS654	
X860de, X862de, X862dte, X864de, X864dhe, XS860, XS862, XS864	
W850n, W850dn, WS850	
T656, TS656	
X746de, X748de, X748dte, XS748	3.X
C748, CS748	
X792de, X792dte, XS795, XS796, XS796, XS798	
C792e, C792de, C792dte, C792dhe, CS796	
X925de, XS925	
C925de	
X950de, X952de, X952dte, X954de, X954dhe, XS950, XS955	
C950de	
X548dte, XS548	
6500e	
MS610, M3150	4.X
MS810, M5155	
MS812, M5170	
CS510	
MX41x, MX51x, XM1145	
MX61x, XM3150	
MX710, XM5163	
MX711, XM5170	
MX81x, XM7155, XM7163, XM7170	
CX41x	
CX51x, XC2132	

To verify if the applications are already installed on the MFP, follow the steps below:

1. Open the embedded Web server (EWS) for the MFP and log in with the user name and password of the device.
2. Select the **Settings** option.
3. Select **Apps**. AC Lexmark Applications version numbers are shown in the printers list of installed applications.

Figure 5-32 Lexmark application




5.10.1 Install HP Access Control (HP AC) Lexmark Applications

- IMPORTANT:** Before installing the solution on Lexmark devices, make sure the correct installation folder displays in the **Installation folder** field in the **Settings** tile > **Agent** tab.
- NOTE:** Lexmark printers need to have Basic secure disabled to install software remotely. You may re-enable security after the install has finished.
- NOTE:** Make sure the printers do NOT have any RFIdeas card readers plugged in prior to installing the software. Drivers will need to be installed, and on some printers the presence of the card reader will prevent the install from completing.
- NOTE:** Alternatively, the *.fls packages may be installed using an anonymous FTP connection to the printer.

1. In the Devices tile, select the Lexmark printer from the device list.
2. Click the **Install** button.

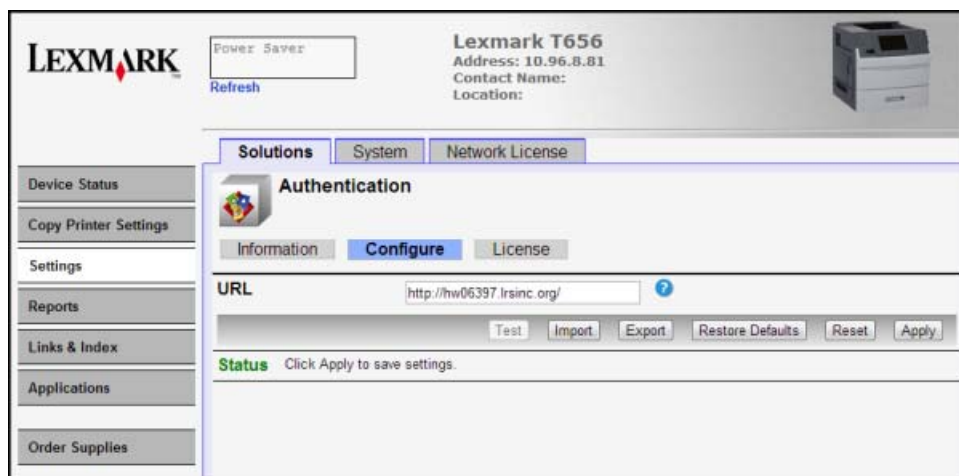
Please wait a few minutes for the AC Lexmark Applications solution to install. To check the status of the printer, go to the printer's EWS. The current status of the device displays in the page header. If the status is "Busy" or "Not Ready", the applications are installing.

5.10.2 Configure AC Lexmark Applications

 **NOTE:** The administration pages may vary, depending on the model of the Lexmark printer.

Configuration of the AC Lexmark Applications solution consists of pointing the AC Authentication and the Card Enroll applications to the AC server. Follow the steps below:


1. In the Devices tile, right-click the Lexmark printer and select **Go to printer ews**.
2. On the printer admin page, select Settings.
3. Select **Apps** or **Embedded Solutions**, depending on the firmware version installed, to view the list of installed applications.
4. Select the **Authentication** solution.
5. Select **Configure**.
6. Update the **AC Server URL** with the appropriate server address. Click **Apply**.




7. Repeat this process for the **Card Enroll** application.

5.10.3 Lexmark device security settings

Configuration of the Lexmark security settings allows the AC server to control what on-device applications a user has access to.

 **NOTE:** Since setting up security on a device is a lengthy process it is recommended that system administrators look into device cloning and other administration tools available from Lexmark.

 **NOTE:** If users encounter authorization problems, users will have to logout and re-authenticate. This issue occurs only when a user authenticates and is properly authorized in one application then attempts to access another application.

1. In the Devices tile, right-click the Lexmark printer and select **Go to printer ews**.
2. On the printer admin pages, select **Settings**.
3. Select **Security**, then select **Security Setup**.
4. If you want to use Card Enroll, select **Active Directory** to configure based on your environment. An HTTPS connection to the EWS may be required. The printer may also automatically reboot in order to join the domain.
5. Select **Security Template**, then click **Add a Security Template**.
6. Enter the name “AC Auth” or similar. Select the AC Authentication setup.
7. If you want to use authorization features, select **Add Authorization**. Select **AC Authentication**.
8. Click **Save Template**.
9. If you want to use Card Enroll, you must set up the Active Directory features and add an Active Directory security template. The Active Directory features may also be named Kerberos, depending on the printer.
10. Click **Return to Security Setup**.
11. Select **Access Controls**.
12. Set up the App/Solution 1-4 to use the **AC Auth** security template.
13. Set up the App/Solution 5 to use the **Active Directory** security template.

See the table below to determine which printers are supported.

Lexmark Security Name	Associated AC Lexmark Application
App 1	AC Express
App 5	Card Enroll

5.10.4 Using the AC Lexmark applications

Prerequisites:

- An RFIDEas RDR-80583AKU card reader must be connected to the MFP if card based authentication is used.
- AC Authentication must be installed and configured on the device.
- Device security settings must be properly configured. At a minimum, an authentication method must be selected for the application you want to use.
- The user must have a card enrolled.

Users can follow the steps below to use a card reader to authenticate at the MFP front panel.

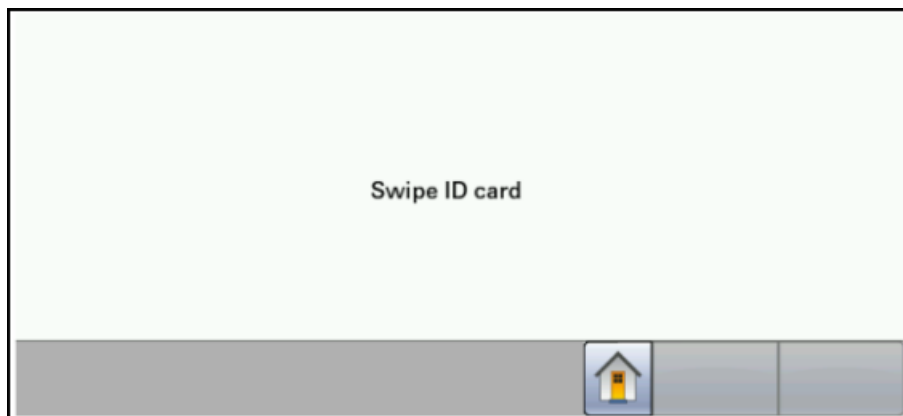
1. Touch the **AC Express** application button.

Figure 5-33 Lexmark welcome



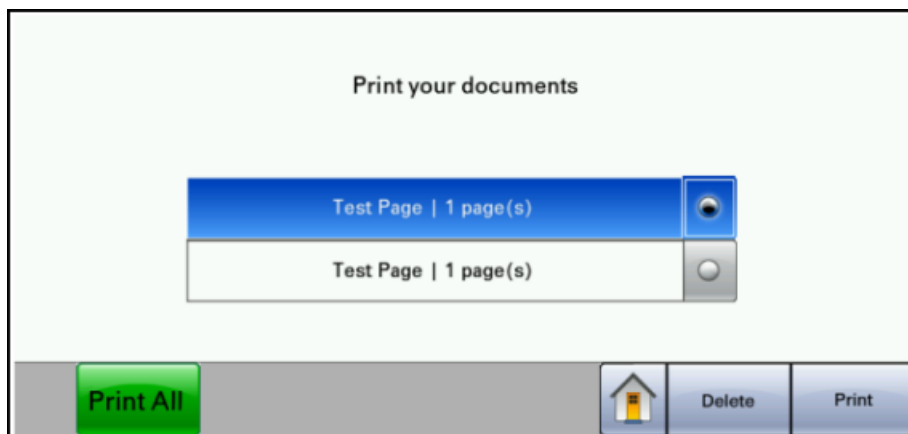
2. Present your proximity card at the card reader for scanning.

Figure 5-34 Lexmark swipe



3. Follow the on screen prompts to authenticate.
4. Follow the on screen prompts to complete the requested action.

Figure 5-35 Lexmark select



5.11 Install and configure components on Xerox devices

Before the AC Express application can be used on the Xerox MFP front panel, MFP devices must have the AC Xerox Agent installed and enabled. This Xerox EIP solution allows applications to be server-based, giving the Xerox MFP the ability to display the menus and communicate with the jobs folder on the servers, without having any components residing directly on the MFP.

See the table below to determine which printers are supported.

Table 5-2 Supported printers

Model	EIP Version version
ColorQube 8700S, 8700X, 8700XF	2.0
ColorQube 8900X	
ColorQube 9301, 9302, 9303	
WorkCentre 5735, 5740, 5745, 5755, 5765, 5775, 5790	
WorkCentre 5865, 5875, 5890	
WorkCentre 7220, 7220T, 7225, 7225T	
WorkCentre 7525, 7530, 7535, 7545, 7556	
WorkCentre 7830, 7835, 7845, 7855	

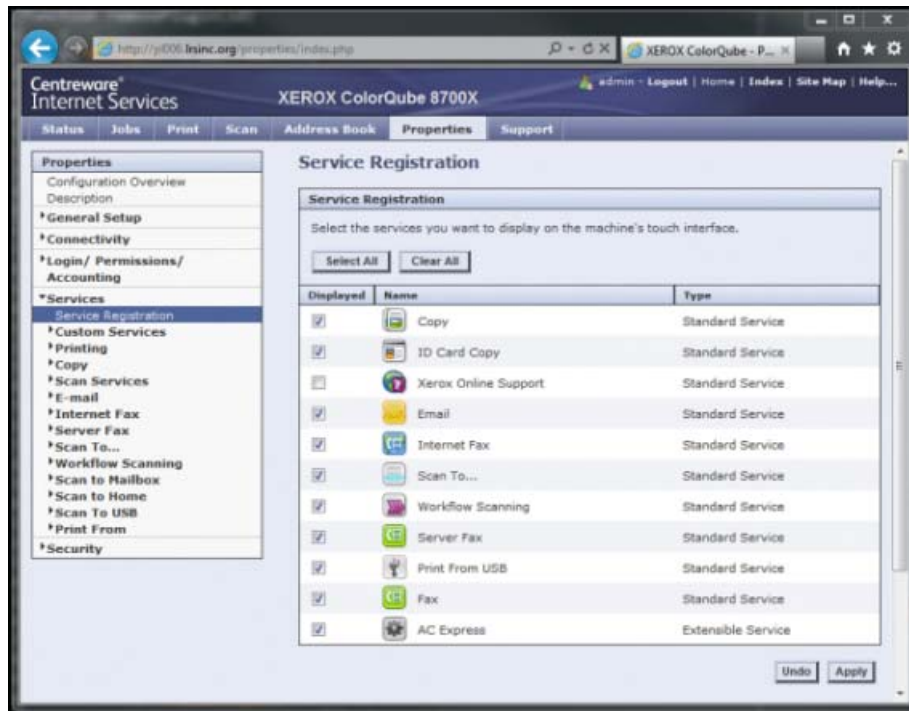
To verify if AC applications are already installed on the MFP, follow the steps below:






NOTE: The administration pages may vary, depending on the model of the Xerox printer.

1. Open a web browser, navigate to <https://servername/XeroxAppsWS/Default.aspx>, where servername is the server address the SPPE application was installed. The page should display “Xerox applications are installed”.
2. Open the embedded Web server (EWS) for the MFP and log in with the user name and password of the device.
3. Select **Properties > Service > Service Registration** and the list contained should display “AC Express.”

Figure 5-36 Xerox application



5.11.1 Configure AC Xerox Applications

-  **NOTE:** Different models of Xerox printers may have different administration pages and these steps may not be completely accurate.
-  **NOTE:** HTTPS is required for communication on the web server and all printers.
-  **NOTE:** Before configuring, make sure the device password matches the password in the **Settings** tile > **Device** tab.

Configuration of the AC Xerox Applications consists of setting up Xerox Secure Access security on your device. The following steps will guide you through the process.

1. In the Devices tile, select the Xerox printer from the device list. Click the **Configure** button. Then select **Pull printing**. Click **OK**. Please wait a few seconds for the AC Xerox Applications solution to register and display on the printer.
2. Right click on the selected printer and select **Go to printer ews**.
3. On the printer admin pages select **Index > Login Methods**.
4. Edit the **Touch UI Method** to use **Xerox Secure Access**, and set any other options to validate on the device.
5. Select **Save**.
6. Click on the **Edit** action next to Xerox Secure Access Setup.
7. Select **Manually Override Settings**.
8. Update the Hostname with the address of the SPPE server (ac.company.org).
9. Update the Path to the correct path of the secure access service (normally "/XeroxAuthWS/SecureAccess.asmx").

10. Change the authentication window title and description as desired, and save.
11. Select **Index > User Permissions** to lock the Xerox Applications to only allow logged in users. This step differs greatly depending on the device and firmware version.

5.11.2 Using the AC Xerox Applications

Prerequisites:

- An RFIDeas RDR-80581AKU card reader with hardware ID VID_OC27&PID_3BFA&REV_1040 must be connected to the MFP if card based authentication is used.
- The user must have a card enrolled.

Users can follow the steps below to use a card reader to authenticate at the MFP front panel.

1. Touch the AC Express application button you would like to use.

Figure 5-37 Xerox welcome



2. Present your proximity card at the card reader for scanning.
3. Follow the on screen prompts to authenticate.
4. Follow the on screen prompts to complete the requested action.

Figure 5-38 Xerox documents



5.12 Configure XT devices

Prerequisites:

- Agent and Secure Pull Print Express must be installed on the server.
- Make sure the XT device is connected to a printer and to the network.
- If your server has a firewall, make sure TCP 2000 is open to send configuration files.
- If your server has a firewall, make sure UDP 11000 port is open for device discovery.
- Make sure the IRM authentication method is set to Card Only.
- Make sure the IRM Proximity Reader settings and Card settings are correct. Also, make sure Card ID masking is enabled.



NOTE: After the card type configuration changes, the XT device must be rebooted or power cycled. To power cycle the XT device, unplug the power cord from the device and then re-plug the power cord.

Follow the steps below:

1. Select the XT device from the device list, then click **Configure**.
2. In the Configure window, select **Pull printing**. Click **OK**.

The device reboots and then beeps five times, indicating the device is configured.

5.12.1 Pull print using XT card readers

Prerequisites:

- The XT device is connected to a printer and the network.
- The XT device is configured.
- Cards are registered to users.

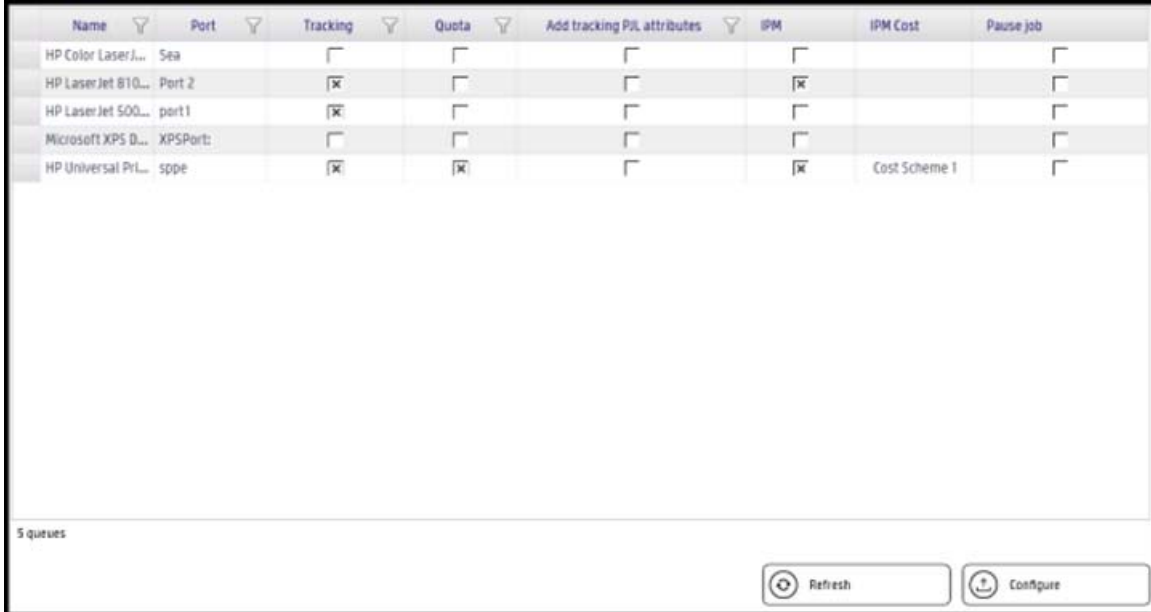
Follow the steps below:

1. Present your registered card at the XT card reader. The XT device identifies the registered card, authenticates the user, and locates your stored jobs in the spool folder. All of your stored jobs are then pulled from the spool folder, printed, and then deleted.
2. Collect your printed documents.

6 Print server tile

The Print Server tile displays all print queues installed on the server, allowing you to configure print queues for tracking, quota or IPM. The columns may vary, depending on if Job Accounting, IPM or both are installed. The checkboxes under the columns indicate what features are enabled for the print queue.

Figure 6-1 Print server tile



Name	Port	Tracking	Quota	Add tracking PJI attributes	IPM	IPM Cost	Pause job
HP Color LaserJet...	Sea	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
HP LaserJet 810...	Port 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>
HP LaserJet 500...	port 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Microsoft XPS D...	XPSPort:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
HP Universal PCL...	sppe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cost Scheme 1	<input type="checkbox"/>

5 queues

Refresh Configure

 **NOTE:** The Print Server tile displays if Job Accounting or IPM is installed.

To configure a print queue, select a print queue from the installed print queues list, then click **Configure**. In the Configure window, select features to enable. Click **OK**.

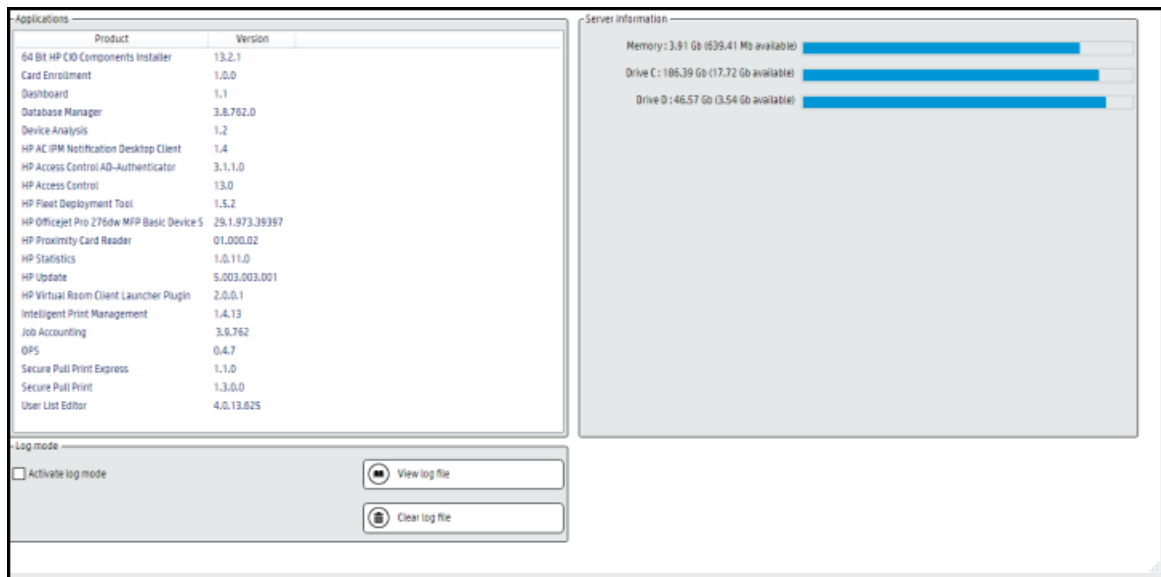
The Configure window displays the following possible features:

- **Tracking:** Enables tracking of print jobs sent to the selected print queue. The print queue tracking method can be either Port Monitor or Print Processor, depending on what is selected in the **Settings** tile > **Print Server** tab.
- **Quota:** Enables the enforcement of Job Accounting quotas for printing.
- **IPM:** Enables the implementation of IPM rules and costs. Select a cost per page scheme from the dropdown list. The cost per page schemes can be set in the **Settings** tile > **IPM** tab. The IPM Cost column displays the cost per page scheme assigned to the selected print queue. For more information about IPM rules and costs, see the *HP Access Control (HP AC) IPM Admin Guide*.
- **Add tracking PJI attributes:** Inserts Job Accounting PJI attributes in the data stream. If an application generates a data stream that does not include the PJI header containing the user and job information, the user and job name are reported as UNSPECIFIED in Job Accounting reports.
- **Pause job:** Automatically pauses print jobs in the print queue. This feature is only possible when Port Monitor is selected for print queue tracking and the Windows service HP ACJASpool Monitor is started.

7 Server Information tile

The **Server Information** tile displays valuable information to help you manage HP Access Control (HP AC) on your server. This tile displays version numbers of installed components, storage and memory of the server, and the HP Access Control (HP AC) log. This makes it easy to check if your HP Access Control (HP AC) components are up to date and view valuable information about your server such as hard drive space available. Click Help > About to view copyright information about HP Access Control (HP AC).

Figure 7-1 Server Information tile



In the **Applications** section, view the list of installed components and version numbers. The Version column lists the versions of the components installed on your server.

In the **Server Information** section, the memory and hard drive storage of the server displays. Use this information to manage your storage and memory space.

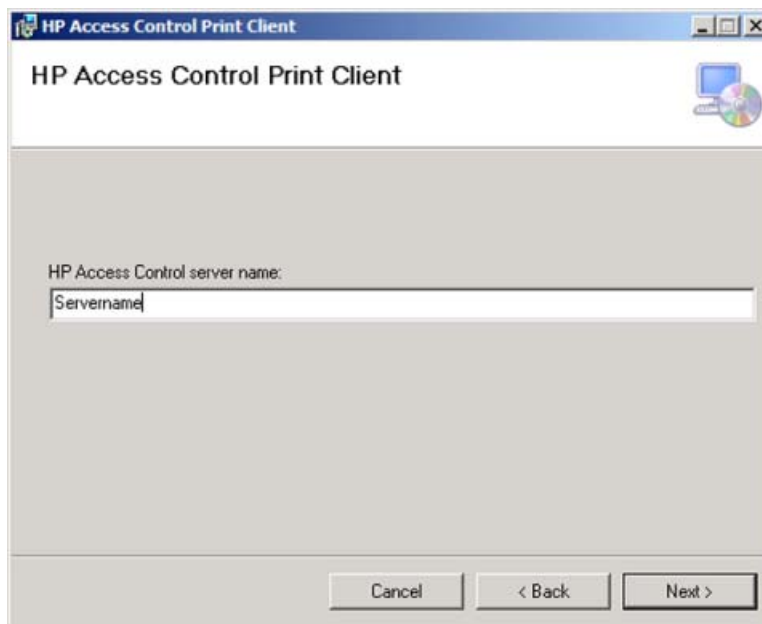
In the **Log mode** section, click the Activate log mode checkbox to enable the log to be created. The log tracks all activity and changes within HP Access Control (HP AC). Click **View log file** to open the log.

8 HP Access Control (HP AC) Print Client

The HP AC Print Client can be installed on client computers to automatically configure installed printers to use IPM rules and Quota. The HP AC server requires IPM and/or Job Accounting to be installed. The HP AC Print Client applies to all currently installed TCP/IP and LPD printers on the client computer. Follow the steps below:

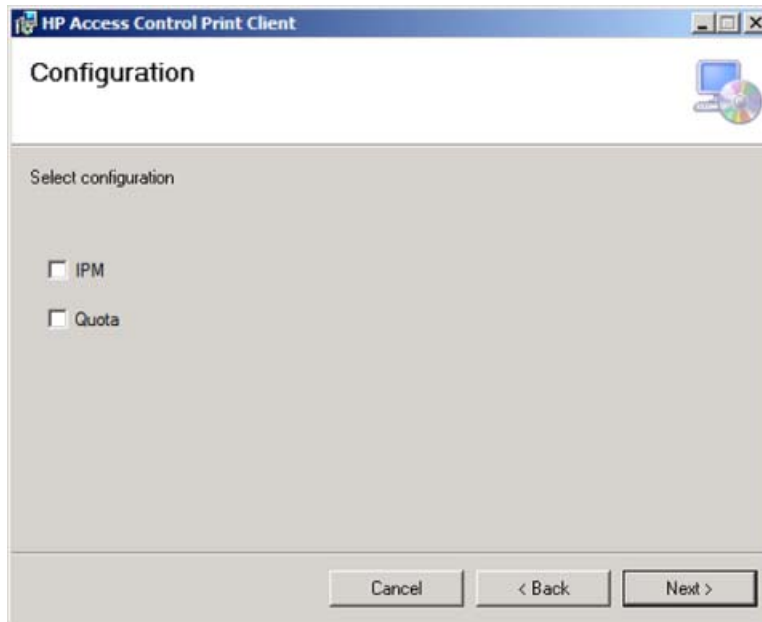
1. Copy the Print Client setup file from the server (located in C:\Program Files\Hewlett-Packard\HP Access Control\client setup\Print client) to the client computer, then run the Print Client setup file.
2. Follow the instructions in the setup wizard. When prompted, enter the name or IP address of the HP AC server with IPM and/or Job Accounting installed. Click **Next**.

Figure 8-1 HP AC Print Client connection



3. On the Configuration screen, select which components you want to configure on installed printers. Select **IPM** to apply the IPM rules from the HP AC server to installed printers on the client. Select **Quota** to apply quota rules from the HP AC server to installed printers on the client. Click **Next**.

Figure 8-2 HP AC Print Client configuration



4. After the installation is complete, click **Close**.